



CCAM TRUST & RESILIENCE

D7.2

Dissemination, Communication, Clustering and Exploitation activities

Project number	101069688
Project acronym	CONNECT
Project title	Continuous and Efficient Cooperative Trust Management for Resilient CCAM
Start date of the project	1 st September 2022
Duration	36 months
Call	HORIZON-CL5-2021-D6-01-04

Deliverable type	R
Deliverable reference number	D6-01-04/ D7.2/ V1.1
Work package contributing to the deliverable	WP7
Due date	Feb 2024 – M18
Actual submission date	29 th February 2024

Responsible organization	FSCOM
Editor	Peter Schmitting
Dissemination level	PU
Revision	1.1 (disclaimer updated)

Abstract	This deliverable presents the CONNECT dissemination, communication, clustering, standardization, and exploitation activities up to M18. Furthermore, it contains information highlighting open-source contributions and workshop organization activities.
Keywords	Communication, Dissemination, Collaborative Tools, Infrastructure, Website, Homepage, Internal Communication, Clustering, Standardization, Open Source, Exploitation, IPR

Editor

Peter Schmitting (FSCOM)

Contributors (ordered according to beneficiary numbers)

Michael Käfinger (TEC)

Thanassis Giannetsos (UBITECH)

Ioannis Krontiris (HUAWEI)

Antonio Kung, Guillaume Mockly, Estíbaliz Arzoz Fernández (TRIALOG)

Francesca Bassi (IRTSX)

Panagiotis Pantazopoulos (ICCS)

Chris Newton (SURREY)

Frank Kargl (UULM)

Disclaimer

The information in this document is provided “as is,” and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

The present deliverable has the objective to provide an update on the WP7 'Dissemination, Standardization, Exploitation & Impact Creation' activities of the CONNECT project. It is the second deliverable in WP7 and follows D7.1 'Plan for Dissemination and Exploitation incl. Communication' [3] which was published in month 6 and describes the dissemination, communication, clustering, standardization, and exploitation activities that took place in the first 18 months of the project and summarizes future plans.

WP7 is comprised of 5 tasks and one chapter is dedicated to each of them with an extra chapter describing the planning for project workshops and presence at conferences.

Task T7.1 'Dissemination and Communication Strategy' covers the dissemination and communication strategy of the CONNECT project. The activities in the continuation of the CONNECT dissemination and communication activities up to month 18 following the plan established in D7.1 [3] are also presented.

Task T7.2 'Contributions to Clusters, 5GAA Interaction and Marketplaces' and T7.3 'Standardization & Regulation Activities' are devoted to project's active participation in activities organized by clusters/associations and standardization organizations relevant to the CONNECT topics. Project partners have been involved in the activities of the cluster organizations CCAM Association and Partnership, CAR 2 CAR Communication Consortium, AIOTI and IDSA and has also contributed to the FAME and GAIA-X projects. In standardization, activities focused on ISO TC204 and JTC1 working groups and on the ETSI committees TC ITS and ISG MEC. Furthermore, contributions to ETSI conferences have been successfully achieved.

Task 7.4 'Open-Source Plan for CCAM Trust Reference Implementation' and Task 7.5 'Exploitation, IPR Handling & Business and Sustainability Planning' are covered in two separate chapters. Chapter 5 defines templates to be completed by CONNECT partners providing artefacts to the project. Chapter 6 then holds a partner-filled table documenting the partners' exploitation plans highlighting changes since the project start.

A final chapter is dedicated to the planning of workshops and the presence of CONNECT at conferences and exhibitions. Currently, it is planned to host a CONNECT workshop collocated with the project's final event and to be present at the ITS World Congress in Dubai (16 – 20 September 2024) with a Special Interest Session and potentially also with a shared stand presence. Furthermore, a presence at the EUCAD conference in Ispra (13 -15 May 2025) is under consideration.

A final report on the dissemination, communication, clustering, and exploitation activities will be provided at the end of the project in month 36 in deliverable D7.3.

Table of Content

Chapter 1	Introduction	1
1.1	CONNECT concept and approach	1
1.2	Purpose of the deliverable	1
1.3	Relation To Other WPs and Deliverables.....	1
1.4	Deliverable Structure.....	2
Chapter 2	Dissemination, communication	3
2.1	Dissemination plans	3
2.2	Dissemination and Communication tools and channels	6
2.3	Past and planned scientific publications.....	12
2.4	Past and planned presentations, conferences, and events.....	15
2.4.1	Highlights.....	15
2.5	Project website.....	18
2.5.1	Social media.....	19
Chapter 3	Clustering.....	21
3.1	Introduction	21
3.2	5GAA	21
3.3	CCAM	22
3.3.1	CCAM Association.....	22
3.3.2	CCAM Partnership.....	23
3.4	CAR 2 CAR Communication Consortium.....	24
3.5	AIOTI.....	24
3.6	Data spaces community.....	25
3.6.1	General.....	25
3.6.2	PrepDSpace4Mobility	25
3.6.3	IDSA.....	26
3.6.4	FAME	26
3.6.5	GAIA-X.....	27
Chapter 4	Standardization	28
4.1	Introduction	28
4.2	Contribution to ISO.....	28
4.2.1	TC204 (Intelligent Transport Systems).....	28
4.2.2	JTC1 SC27 (Cybersecurity and privacy)	30
4.2.3	JTC1 SC41 (IoT and Digital Twins).....	31
4.3	Contributions to ETSI	32
4.3.1	TC ITS (Intelligent Transport Systems)	32
4.3.2	ISG MEC (Multi-access Edge Computing).....	32

4.3.3	ETSI security conference 2023.....	33
4.3.4	ETSI IoT conference 2023.....	35
4.4	Trusted Computing Group (TCG).....	35
Chapter 5	Open-source Contributions.....	37
Chapter 6	Exploitation, Business and Sustainability Planning	52
Chapter 7	Workshop planning.....	54
Chapter 8	Summary and Conclusion	56
Chapter 9	List of Abbreviations.....	57
Chapter 10	References	59
Appendix A	CONNECT Open-Source Project Plan Template	61

List of Figures

Figure 1: CONNECT Pert chart.....	2
Figure 2:Nataša Trkulja from Ulm University on the topic of "In-vehicle Trust Assessment Framework.".....	16
Figure 3: First CONNECT newsletter: LINK	16
Figure 4: Interview Alexander (Denso) LINK	17
Figure 5: Technical meeting Munich: LINK	18
Figure 6: Website statistics CONNECT.....	19
Figure 7: X-Statistics.....	19
Figure 8: LinkedIn statistics.....	20
Figure 9: LinkedIn statistics per entry.....	20
Figure 10: The seven CCAM clusters.....	23
Figure 11: CONNECT presence at ETSI Security conference.....	33
Figure 12: CONNECT poster at ETSI Security conference.....	34
Figure 13: CONNECT presence at TCG Members Physical Meeting in June 2023.....	35

List of Tables

Table 1: Dissemination plans.....	3
Table 2: Dissemination material.....	6
Table 3: Planned dissemination.....	10
Table 4: CONNECT activities at CCAM Partnership.....	24
Table 5: CONNECT input to ISO TR12786.....	29
Table 6: ISO TR12786 related standardization activities.....	30
Table 7: CONNECT open-source project plan - open-source plan info.....	38
Table 8: CONNECT open-source project plan – context.....	39
Table 9: CONNECT open-source project plan – strategy.....	41
Table 10: CONNECT open-source project plan – engagement.....	43
Table 11: CONNECT open-source project plan - project development.....	43
Table 12: CONNECT open-source project plan - evaluation and approval of plan.....	51
Table 13: Industrialization efforts per CONNECT partner.....	53
Table 14: Target events for CONNECT participation.....	55
Table A1: Open-source project plan – open-source plan info.....	61
Table A2: Open-source project plan – context.....	62
Table A3: Open-source project plan - strategy.....	65
Table A4: Open-source project plan – engagement.....	66
Table A5: Open-source project plan - project development.....	67
Table A6: Open-source project plan - evaluation and approval of plan.....	67

Chapter 1 Introduction

1.1 CONNECT concept and approach

The vision of the CONNECT project is to address the convergence of security and safety in CCAM by assessing dynamic trust relationships and defining a trust model and trust reasoning framework based on which involved entities can establish trust for cooperatively executing safety-critical functions. The CONNECT Trust Management framework is the basis that models and captures the trust relationships of the next generation CCAM systems. CONNECT's new safety paradigm is a key element in bringing autonomous driving to a completely new level of trustworthiness and is expected to lead to long-term consumer acceptance as a result.

In most cases, there is a certain level of mistrust between entities in terms of safety when it comes to autonomous driving. Beyond the needs of functional safety, trustworthiness management should be included in CCAM's security functionality solution. The project establishes a trust management framework centred on zero-trust paradigms which expands by assessing dynamic trust relationships based on who is involved in providing the information. Combining the vehicle's systems with information available in the cloud and edge, expands the knowledge on the environment required for decision making, outsources the calculations in a trustworthy way to the backend of the cloud and helps in this way to make faster decisions, cooperatively and without delay increasing the safety of autonomous driving. The features of CONNECT facilitating next generation ITS solutions enable it addressing challenges in the era of personal mobility and environmental sustainability.

1.2 Purpose of the deliverable

The purpose of deliverable D7.2 is to provide of an update on the WP7 'Dissemination, Standardization, Exploitation & Impact Creation' activities of the CONNECT project. It is the second deliverable in WP7 and follows D7.1 'Plan for Dissemination and Exploitation incl. Communication' [3] which was published in month 6 and describes the dissemination, communication, clustering, standardization, and exploitation activities that took place in the first 18 months of the project and summarizes future plans. A final report on the dissemination, communication, clustering, and exploitation activities will be provided at the end of the project in month 36 in deliverable D7.3 summarizing the activities in the second half of the project's lifetime.

1.3 Relation To Other WPs and Deliverables

The figure below depicts the relation between the different work packages (WP) in a Pert chart. All WPs feed their results to WP7 which will evaluate them for the purpose of communication, dissemination, and standardization.

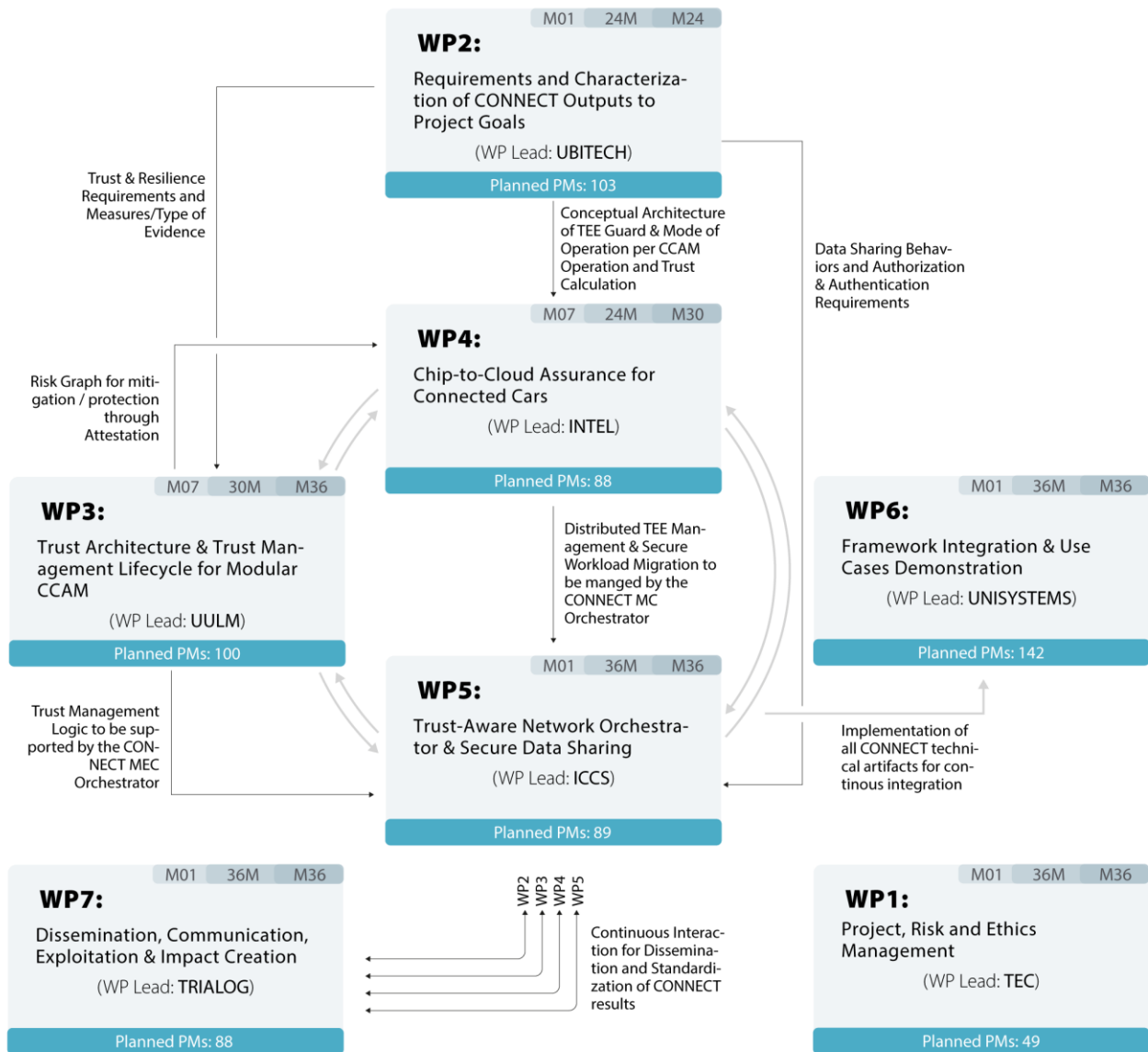


Figure 1: CONNECT Pert chart

1.4 Deliverable Structure

The present deliverable is structured in 10 chapters following the task structure of WP7.

- Chapter 1 contains an introduction to the deliverable.
- Chapter 2 summarizes the dissemination and communication tasks of T7.1 'Dissemination and Communication Strategy'.
- Chapter 3 reports on the partners' activities in industry groups of T7.2 'Contributions to Clusters, 5GAA Interaction and Marketplaces'.
- Chapter 4 reports on the partners' activities in standardization organizations of T7.3 'Standardization & Regulation Activities'.
- Chapter 5 presents a template structure for T7.4 'Open-Source Plan for CCAM Trust Reference Implementation'.
- Chapter 6 lists partner inputs into the exploitation template for T7.5 'Exploitation, IPR Handling & Business and Sustainability Planning'.
- Chapter 7 provides a planning for workshops that will be organized by the CONNECT project.
- Chapter 8 summarizes the main take-aways of the deliverable.
- Chapter 9 contains the list of abbreviations.
- Chapter 10 lists all documents referenced in the text.





Chapter 2 Dissemination, communication

Chapter 2 offers a comprehensive update on the first dissemination report, D7.1 of the CONNECT project. It explains the dissemination and communication initiatives undertaken during the project, while also providing a summary of forthcoming plans.

2.1 Dissemination plans

In the following table, the different dissemination activities that have been planned in the DoA can be observed. Dissemination activities are considered key enablers for the success of the CONNECT project. The goal of dissemination is to make many stakeholders (phase modulation, real-time holography, virtual-/augmented-/mixed-reality) aware of the CONNECT approach and results. Wherever possible, research results will be used for the creation and support of CONNECT outcome and will substantially contribute to the benefit of the targeted constituents (Broad Public Society & Media (A), Policy Makers (B), Industry (C) and Research Community (D)). In the table below, the green tick marks represent activities that are completed/ongoing.

Table 1: Dissemination plans

Type of Activity / Material – Time	Target Groups & Expected Impact	KPI / Means to measure KPI
Phase 1: Awareness creation		
Announcement letter – (C) – <i>Within first 2 weeks of project</i> 	General public, research community and potential stakeholders from industry informed about project start.	5000 people via press releases in public and social media, on project website and on partners' websites
Project website and branding – (C), (D) – <i>2nd month of project</i> 	Interested stakeholders worldwide informed about the project and its results, by publishing news such as conference visits, publications & deliverables, etc. Increased awareness of the project among all target groups; Marketing pack and promotional press kit (Rollup, brochure, banner).	> 1000 unique visitors > 200 registrants > 350 blog interactions
Audio and Video Material – (C), (D) – <i>Throughout pr.</i>  (to be continued)	General public and policy makers aware of main objectives of the project; visually engage/offer Trainings to enable CONNECT's Open-Source Impl. Roadmap (WP7).	1 Promo + 1/Pilot + 1 Impact + 2-4 interviews
Social Media (e.g. Twitter, LinkedIn) – (C), (D) – <i>Throughout pr.</i>  (to be continued)	Strong digital presence, new leads for synergies/liasons - Project activities and results relevant for society presented to general public and policy makers through new media.	> 1000 followers > 800 posts > 5000 interactions

Phase 2: Continuity of information flow		
<p>Press releases, blog posts, articles, whitepapers – (C), (D) – <i>Throughout pr.</i></p> <p style="text-align: center; color: green; font-size: 2em;">✓</p> <p>(to be continued)</p>	<p>Increased awareness among the industry, scientific community, stakeholders, and general public on technological and scientific progress; distribution via public and social media and project website.</p>	<p>> 4/per year (> 1000 people)</p>
<p>Participation in and publication of scientific papers in conferences and high impact factor journals – (D), (E) – <i>Throughout project</i></p> <p style="text-align: center; color: green; font-size: 2em;">✓</p> <p>(to be continued)</p>	<p>Comparison with international research community, potential for international cooperation identified. Project results disseminated and made accessible to research community and industry through Open Access Publications.</p> <p>Conferences: IEEE EuroS&P, IEEE VNC, ACM WiSec, NDSS, ACM CCS, IEEE DCOSS, ESORICS, Asia CCS, IEEE INFOCOM</p> <p>Journals: IEEE TIFS, IEEE Transactions on Mobile Computing, ACM TOPS, IEEE ITS, IEEE TDSC</p>	<p>> 4 Journal articles > 15 Conference papers</p>
<p>Interaction with policy makers – (D), (E) – <i>Throughout project</i></p>	<p>Input provided for discussions and recommendations exchanged among the involved countries;</p> <p>Industry links and synergies; F2F interactions with end-user organizations, Urban Public (through IRTSX partner).</p>	<p>> 6 synergies established with policy makers reached via e-mail or physically</p>
<p>Digital liaisons with related projects – (D), (E) – <i>Throughout project</i></p> <p style="text-align: center; color: green; font-size: 2em;">✓</p> <p>(to be continued)</p>	<p>Feedback exchanged with national, European, and international research projects from the same field (Section 1.2.4) through e-mails, face-to-face meetings, or other means; Organization of joint scientific and industrial workshop to engage the scientific community, related organizations, and automotive stakeholders.</p>	<p>Workshops organized (3) + attended (> 5), > 500 visitors, 10 speakers; 5 posts in CORDIS/other EC systems; 10 project synergies (incl. common product/services by joining project assets)</p>
<p>Non-scientific Publications – (D), (E) – <i>Throughout project</i></p> <p style="text-align: center; color: green; font-size: 2em;">✓</p> <p>(to be continued)</p>	<p>Adoption by the public, Training/Showcases;</p> <p>Open access exhibitions and demonstration events. Show CONNECT use cases to visitors in lively, lightweight manner.</p>	<p>> 5 Industry Magazines > 6 Industrial Automotive Cyber Security Conferences (e.g., ESCAR)</p> <p>1 exhibition 2 demonstration days</p>
<p>Standardization associations - (D), (E) – <i>Throughout project</i></p> <p style="text-align: center; color: green; font-size: 2em;">✓</p> <p>(to be continued)</p>	<p>Interactions with standardization WGs and committees for pushing the core artefacts of CONNECT (Section 2.2.3) related to Security & Safety Convergence, Dynamic Trust Modelling, Chip-to-Cloud Assurance, and Digital Twins, etc. Meeting attendance and common publications.</p>	<p>(EU & International) Automotive > 3, Transport/Mobility > 3, Standards Orgs > 4</p>

Phase 3: Result orientation		
On-site Pilot Demonstrations/ Workshops – (D), (E) – <i>Throughout pr.</i>	Automotive service providers, vehicle manufacturers, traffic and transport industry attracted; short video media coverage.	> 1 demonstration per pilot > 2 workshops per pilot > 30 attendees each
Online and/or F2F Training/Webinars – (D) – <i>Throughout project</i>	Training activities will be organized during the project involving both internal and external members of the project. One of the goals is to mitigate the gap that typically separates practitioners and theoreticians by providing a series of regular structured training events.	> 2 webinar/trainings > 50 attendees
CONNECT Day – (D) – <i>Towards project end</i>	Project results and future work presented to stakeholders from automotive industry and research community. Speakers working on related topics invited.	> 80-100 participants

2.2 Dissemination and Communication tools and channels

The CONNECT project already provided a certain number of dissemination materials that is summarized in table underneath.

Table 2: Dissemination material

Type of activities	Main Leader	Other partners	Title	Date	Place	Type and goal of the event / website
Participation to a Conference	UULM	DENSO	Symposium on Cryptography and Information Security (SCIS) 2023	24.01.2023-27.01.2023	Kokura, Japan	General promotion of the CONNECT project to the research community
Website	TEC	UULM, HUAWEI	Fact Sheet 1: Trust Assessment	02.03.2023	Online	Detailed information and animated graphic; as blog, pdf and via social media
Video/Film	TEC	All partners	Women in Technology: Celebrating the Women of the CONNECT project	08.03.2023	Online	International Women's Day https://www.linkedin.com/feed/update/urn:li:activity:7038974074001207296
Participation to a Workshop	UBITECH	HUAWEI	IEEC Vehicular Networking Conference VNC	26.04.2023-28.04.2023	Istanbul, Turkey	Presentation of a paper: Comparative Evaluation of PKI and DAA-Based Architectures for V2X Communication Security” by A. Angelogianni, I. Krontiris, and T. Giannetsos
Organization/ Participation of/in a Conference	UULM	DENSO	IEEC Vehicular Networking Conference VNC	26.04.2023-28.04.2023	Istanbul, Turkey	Co-Organization of conference by UULM, presentations by partners and paper published.
Other	TEC	UBITECH	Contribution to EC CINEA publication (publication date)	03.05.2023	Online	CONNECT project introduction: Contribution to project presentations on "Towards Cooperative, Connected & Automated Mobility" published by CINEA

Type of activities	Main Leader	Other partners	Title	Date	Place	Type and goal of the event / website
						https://cinea.ec.europa.eu/publications/towards-cooperative-connected-and-automated-mobility_en
Website	TEC	UTWENTE	Fact Sheet 2: Trust relationships	04.05.2023	Online	https://horizon-connect.eu/wp-content/uploads/2023/07/CONNECT_Fact_Sheet.pdf
Video/Film	TEC		CONNECT explainer video	15/05/2023	Online	https://horizon-connect.eu/connect-explained/
Social media	TEC	CRF, POLITO, IRTSX, DENSO	Use case introduction	15/05/2023	Online	Interviews with Use Case Partners introducing the CONNECT use cases. https://horizon-connect.eu/blog/
Participation to a Workshop	FSCOM		ISO TC204 61th plenary, focus on WG20 "Big Data and Artificial Intelligence supporting ITS", WG19 "Mobility integration" and WG17 "Nomadic Devices in ITS Systems"	15.05.2023-19.05.2023	San Antonio, USA	Promote CONNECT Use case in TR12786, awareness raising for CONNECT activities and potential candidates for standardization
Organization/ Participation of/in a Conference	HUAWEI, UBITECH	UULM, DENSO	ITS European Congress 2023 Panel: Roadmap towards adoption of dynamic trust assurances for sustainability in CCAM	22/05/2023-23/05/2023	Lisbon, Portugal	Organization and participation in an experts panel https://itseuropeancongress.com/programme-daily-overview/ .

Type of activities	Main Leader	Other partners	Title	Date	Place	Type and goal of the event / website
Video/Film	TEC	IRTSX	Interview presented Use case 1	23.05.2023	Online	Vimeo video, blog, and social media
Participation to a Conference	SURREY	TEC, UBITECH	Poster presentation at ACM WISEC 2023	29.05.2023-01.06.2023	Guilford, Surrey, UK	Poster "Connect Roadmap Towards Adoption of Dynamic Trust Assurances for Sustainability in CCAM" ACM WISEC 2023 - https://wisec2023.surrey.ac.uk/
Organization of a Workshop	UULM, HUAWEI		Dagstuhl Seminar Dagstuhl Seminar 23242	11.06.2023-16.06.2023	Dagstuhl, Germany	Privacy Protection of Automated and Self-Driving Vehicles https://www.dagstuhl.de/en/seminars/seminar-calendar/seminar-details/23242
Participation to a Conference	UULM		IEEE Vehicular Technology Conference VTC Spring	20.06.2023-23.06.2023	Florence, Italy	Paper published and a presentation given - https://events.vtsociety.org/vtc2023-spring/
Participation to a Workshop	UBITECH		Trusted Computing Group (TCG)	29.06.2023	Berlin, Germany	Presentation on vision of CONNECT
Video/Film	TEC	DENSO	Interview presented Use case 2	03.07.2023	Online	Vimeo video, blog, and social media
Website	TEC	UTWENTE	Fact Sheet 2: Trustworthiness	05.07.2023	Online	Presented in leaflet format, as blog, pdf and via social media

Type of activities	Main Leader	Other partners	Title	Date	Place	Type and goal of the event / website
Participation to a Conference	SURREY		PCCrypto Conference	13/08/2023-16/08/2023	Maryland , US	https://pccrypto2023.umiacs.io/
Participation to other events	POLITO		Hi-drive summer school	06/09/2023-07/09/2023	Porto Cheli, Greece	Presentation on vision of CONNECT for Day-2 and beyond V2X services
Participation to a Workshop	FSCOM		ISO TC204 60th plenary, focus on WG20 "Big Data and Artificial Intelligence supporting ITS"	03.10.2022-07.10.2022	Tampere , Finland	Promote CONNECT Use case in TR12786
Participation to a Conference	IRTSX	HUAWEI, UBITECH, FSCOM	ETSI Security Conference - Presentation and Poster	16/10/2023-19/10/2023	Sophia Antipolis, France	Presentation abstract submitted, Poster to be submitted later. http://www.etsi.org/etsisecurityconference
Participation to a Workshop	POLITO		Towards The Sustainable Vehicle Era Workshop	14/11/2023-15/11/2023	Turin, Italy	The event is dedicated to important emerging technologies: speakers from industry and academia will intervene in two sessions, titled "Future Trends in Low Emission Vehicles" on November 14 and "Automated and Connected Vehicles" on November 15. On both days there will be an exhibition of prototypes and visits to the CARS - Centre for Automotive Research and Sustainable Mobility laboratories and PEIC - Power Electronics Innovation Centre.
Participation to a Conference	UULM		escar Europe	15/11/2023-16/11/2023	Hamburg , Germany	Co-organizer, paper published, and a presentation given, networking with community, discussions about trust modelling, advertising CONNECT project

Type of activities	Main Leader	Other partners	Title	Date	Place	Type and goal of the event / website
Participation to a Conference	SURREY		ICICS 2023	18/11/2023-20/11/2023	Tianjin, China	Presentation of DRoT: A Decentralised Root of Trust for Trusted Networks
Participation to a Conference	UULM		Italian Networking Workshop	22/01/2024-24/01/2024	Madonna di Campiglio, Italy	Presentation of a keynote on “Putting Trust in Networks” introduces CONNECT and Trust Assessment Framework to audience of 150 researchers.
Participation to a Conference	HUAWEI		RTR Conference	05/02/2024	Brussels	Presentation of the CONNECT project at the Trustworthiness CCAM session

In the months ahead, the CONNECT team will persist in raising awareness about the project through its website, blog, and various social media platforms. This phase, particular emphasis will be placed on maintaining a consistent flow of information, with a heightened focus on press releases, blog posts, articles, whitepapers, engagement with policymakers, and digital collaborations with related initiatives such as the CCAM's Network, as well as with standardization associations. During this phase, considerable attention has been directed towards actively participating in conferences and continuing of publishing scientific papers in high-impact journals. Collaborating with various partners, the team aims to present CONNECT's key concepts and initial findings through scientific publications and presentations, further solidifying its presence in the academic and research community.

Table 3: Planned dissemination

Type of activities	Main Leader	Other partners	Title	Start	Place	Type and goal of the event / website
Website	TEC	ALL	2 nd Newsletter	April	Online	Newsletter
Participation to a Conference	UULM	HUAWEI, UBITECH, IRTSX	30th ITS World Congress	16 – 20 September 2024	Dubai	ITS World Congress in Dubai 2024

Participation to a Conference	UULM; HUAWEI, UBITECH		Conference on Connected and Automated Driving	13-15 May 2025	Ispra (Italy)	EUCAD 2025 - Connected Automated Driving
Participation to a Conference	UULM		VehicleSec 2024	26 February 2024	San Diego, CA	https://www.ndss-symposium.org/ndss2024/co-located-events/vehiclesec/
Participation to a Conference	UULM		Escar Europe 2024	18 – 20 November 2024	Dortmund, Germany	https://escar.info/escar-europe/

2.3 Past and planned scientific publications

During the second period of the project, CONNECT has submitted 11 papers at conferences that were accepted:

Title: Securing Cooperative Intersection Management through Subjective Trust Networks

Link to paper: <https://ieeexplore.ieee.org/document/10200789>
<https://horizon-connect.eu/scientific-publications/>

Conference: IEEE VTC Spring 2023

Authors: Frank Kargl, Nataša Trkulja, Artur Hermann, Florian Sommer, Anderson Ramon Ferraz de Lucena, Alexander Kiening, Sergej Japs

Abstract: Connected, cooperative, and autonomous mobility (CCAM) will take intelligent transportation to a new level of complexity. CCAM systems can be thought of as complex Systems-of-Systems (SoS). They pose new challenges to security as consequences of vulnerabilities or attacks become much harder to assess. In this paper, we propose the use of a specific type of a trust model, called subjective trust network, to model and assess trustworthiness of data and nodes in a SoS. Given the complexity of the topic, we illustrate the application of subjective trust networks on a specific example, namely Cooperative Intersection Management (CIM). Therefore, we introduce the CIM use-case and show how it can be modelled as a subjective trust network. We then analyse how such trust models can be useful both for design time analysis and run-time verification and allow us a more precise quantitative of trust in automotive SoS. Finally, we also discuss the open research problems and practical challenges that need to be addressed before such trust models can be applied in practice.

Title: An ML-Aided Reinforcement Learning Approach for Challenging Vehicle Manoeuvres

Link to paper: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9963702>
<https://horizon-connect.eu/scientific-publications/>

Conference: IEEE TRANSACTIONS ON INTELLIGENT VEHICLES

Authors: Dinesh Cyril Selvaraj, Shailesh Hegde, Nicola Amati, Francesco Deflorio and Carla Fabiana Chiasserini (POLITO)

Abstract: The richness of information generated by today's vehicles fosters the development of data-driven decision-making models, with the additional capability to account for the context in which vehicles operate. In this work, we focus on Adaptive Cruise Control (ACC) in the case of such challenging vehicle manoeuvres as cut-in and cut-out and leverages Deep Reinforcement Learning (DRL) and vehicle connectivity to develop a data-driven cooperative ACC application.

Title: ZEKRA: Zero-Knowledge Control-Flow Attestation

Link to paper: <https://doi.org/10.1145/3579856.3582833>
<https://horizon-connect.eu/scientific-publications/>

Conference: ACM AsiaCCS 2023

Authors: Heini Bergsson Debes, Edlira Dushku, Thanassis Giannetsos, Ali Marandi

Abstract: This paper presents a new scheme for attesting the operational correctness of a device's (specific) codebase in a privacy-preserving manner leveraging zSNARKS. This is to be part of CONNECT Attestation Toolkit on verifying such runtime attributes as an indication on the trust level of a vehicle. The interesting questions here to discuss further is how to be able to offload part of this security calculation to the MEC so that we can use the digital twin of each vehicle as a "trusted worker".

Title: DRoT: A Decentralised Root of Trust for Trusted Networks

Link to paper: [https://link.springer.com/chapter/10.1007/978-981-99-7356-9_40#:~:text=\(Decentralised%20Root%20of%20Trust%20\(DRoT,Root%20of%20Trust%20\(DRoT\)\)](https://link.springer.com/chapter/10.1007/978-981-99-7356-9_40#:~:text=(Decentralised%20Root%20of%20Trust%20(DRoT,Root%20of%20Trust%20(DRoT)))

Conference: International Conference on Information and Communications Security (ICICS 2023)

Authors: Parthipan L.; Chen, L.; Newton C.; J. P.; Li Y.; Liu F. and Wang D.

Abstract: For many years, trusted computing research has focused on the trustworthiness of single computer platforms. For example, how can I decide whether I can trust my personal computer (*A*) or another computer (*B*), who communicates with *A*? In reality, both *A* and *B* are part of a computing network, in which there are many other computers, and these computers' behaviour affects the trustworthiness of any communication between *A* and *B*. Obviously, the target of trusted computing is not only to build trusted devices but also trusted networks. Attestation is a mechanism initially designed to ascertain the trustworthiness of a single device. To check on the trustworthiness of a network, we need a network attestation mechanism. The basis of attestation is a root of trust, and research on building roots of trust for individual devices has been successful. One of the next challenges, the most important one, is to create a root of trust for network attestation. In this paper, we introduce our research on designing such a root of trust. This uses devices' individual roots of trust and a decentralised ledger together with the techniques of "zero trust but verify," which means that to start with, any entity in the system is not trusted until its functionality can be verified. Based on the verification results, the entities can establish trust. We aim to use such a root of trust to aggregate the attestation evidence and verification results from multiple devices in a network and to achieve trust in the network.

Title: Roadmap Towards the Adoption of Dynamic Trust Assurances for Safety and Security Convergence in Safety-Critical Systems

Link to paper: <https://hal.science/hal-04253860>.

<https://horizon-connect.eu/scientific-publications/>

Conference: ETSI Security Conference

Authors: Francesca Bassi, Thanassis Giannetsos, Ioannis Krontiris

Abstract: Further Information in chapter 4.3 Contributions to ETSI

Title: Comparative Evaluation of PKI and DAA-Based Architectures for V2X Communication Security

Link to paper: <https://zenodo.org/records/8093399>.

<https://horizon-connect.eu/scientific-publications/>

Conference: IEEE VNC 2023

Authors: A. Angelogianni I. Krontiris, and T. Giannetsos

Abstract: The emerging Cooperative Intelligent Transportation Systems (C-ITS) landscape is expanding in terms of security and trust requirements, to provide the necessary enablers for the safety of critical operations (i.e., collision avoidance). To this extend, Public Key Infrastructure (PKIs) and Direct Anonymous Attestation (DAA) schemes have been proposed by the literature, in order to provide authenticity over the exchanged messages. DAA schemes can help address several challenges of centralized PKIs by offering a more scalable solution for pseudonym certificate reloading and revocation. This paper is the first to implement a DAA-based solution and then do a methodological comparison of the two schemes side-by-side based on an experimental evaluation. The acquired results do not directly dictate one prevailing solution, but rather suggest the need for an integrated approach converging concepts from both schemes, to better accommodate the needs of future C-ITS systems.

Title: The Internet of Vehicles (IoV) — Security, Privacy, Trust, and Reputation Management for Connected Vehicles

Link to paper: <https://ieeexplore.ieee.org/document/10145018>.

<https://horizon-connect.eu/scientific-publications/>

Conference: IEEE Internet of Things Magazine, vol. 6, no. 2, pp. 6-16

Authors: A. Drobot, T. Zhang, M. L. Buonarosa, F. Kargl, S. Schwinke and B. Sikdar

Abstract: The IEEE IoT Magazine hosted a Virtual Roundtable to discuss the technologies, business models, governance regimes, and public perceptions of the challenges and opportunities for solutions to issues of security, privacy, and trust for connected vehicles.

Title: In-vehicle Trust Assessment Framework

Link to paper: <https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/docId/10384>

<https://horizon-connect.eu/scientific-publications/>

Conference: ESCAR Europe 2023

Authors: N. Trkulja; A. Hermann; A. Petrovska; A. Kiening; A. Ramon Ferraz de Lucena, F. Kargl

Abstract: Today's vehicles run various safety-critical applications requiring data input from diverse in-vehicle components. Adaptive Cruise Control (ACC), for example, can rely on the data input from components such as lidar, radar, GNSS, and cameras. Malicious manipulation of any of this data compromises the data integrity and can result in safety incidents or accidents on the road. Security mechanisms like misbehaviour detection can be in place; however, they cannot reliably assess the consequences of attacks on a system level or for arbitrary subsystems. In this paper, we present a Trust Assessment Framework (TAF) that allows an in-vehicle application in a complex System-of-Systems to assess whether it can trust the integrity of its input data. The TAF assesses the trustworthiness of every component in the data flow chain based on collected evidence. We explain this concept with the example of ACC and showcase two possible implementations of the TAF inside a vehicle.

Title: Hash-based Direct Anonymous Attestation

Link to paper: https://link.springer.com/chapter/10.1007/978-3-031-40003-2_21

Conference: PQCrypto 2023

Authors: Chen L.; Dong C.; El Kassem N.; Newton C.J.P. and Wang Y.

Abstract: We propose the first post-quantum DAA scheme from symmetric primitives. We make use of a hash-based signature scheme, which is a slight modification of SPHINCS+, as a DAA credential. A DAA signature, proving the possession of such a credential, is a multiparty computation-based non-interactive zero-knowledge proof. The security of our scheme is proved under the Universal Composability (UC) model.

Title: Trust Level Evaluation Engine for Dynamic Trust Assessment with Reference to Subjective Logic

Link to paper: DOI not available yet, accepted and presented.

Conference: IFIPTM2023: The 14th IFIP WG 11.11 International Conference on Trust Management

Authors: Ana Petrovska, Gabriele Gelardi, Hüseyin Demirci, Emre Kocyigit, Gabriele Lenzini, Artur Hermann, Nataša Trkulja, Frank Kargl, Ioannis Krontiris, and Theo Dimitrakos

Abstract: In this work, we propose an architectural design for a Trust Level Evaluation Engine. The engine is meant to work in a complex and dynamic environment of potentially untrustworthy sources of information where the situational knowledge is partial and subjective from the viewpoint of the information source, thus potentially inconsistent and contradictory; and, consistently with a Zero-Trust approach, no initial trust between nodes should be assumed. Therefore, a decision-making module shall nevertheless figure out its level of confidence about the truth of a proposition over the reality. Our design is theory-agnostic and can be instantiated on different mathematical subjective model theories, but we demonstrate its feasibility by mapping it on the Subjective Logic. In this paper,

we also discuss critical design choices, including algorithmic details that are only partially addressed in the abstract description of the theory, whilst we demonstrate how the engine effectively works on large and complex subjective trust networks. Additionally, we offer a proof-of-concept implementation to showcase the proposed architecture's ability to handle intricate and complex networks.

Title: Edge-assisted ML-aided Uncertainty-aware Vehicle Collision Avoidance at Urban Intersections

Link to paper: <https://ieeexplore.ieee.org/document/10185090>

Conference: IEEE TRANSACTIONS ON INTELLIGENT VEHICLES

Authors: Dinesh Cyril Selvaraj, Christian Vitale, Tania Panayiotou, Panayiotis Kolios, Carla Fabiana Chiasserini, Georgios Ellinas

Abstract: The paper discusses a new approach to address the dangerous nature of intersection crossings in road infrastructure using Connected Vehicles (CVs) and Multi-access Edge Computing (MEC) on 5G networks. The proposed framework involves an Intersection Manager (IM) at the MEC, which gathers information from vehicles and road infrastructure to gain a comprehensive understanding of the intersection. The IM utilizes historical data and an encoder-decoder recurrent neural network to predict future trajectories of vehicles with high accuracy. Additionally, the model incorporates uncertainty measures for confident collision forecasting and avoidance. This uncertainty-aware collision prediction framework can effectively detect potential collisions well in advance and trigger alarms to prompt the colliding vehicles to brake, thereby preventing accidents in real-world scenarios. The approach has been shown to successfully avert simulated imminent dangers.

All publications produced during the project's lifetime except of four are available on the website following the link: <https://horizon-connect.eu/scientific-publications/>.

Currently, there are 3 papers in progress for the upcoming period, with the titles A Trust Assessment Method for In-Vehicular Networks using Vehicle Risk Assessment; RAKIS: Certifying Fast IO Primitives Across Trust Boundaries on Intel SGX; and Gramine-TDX: A Lightweight OS Kernel for Confidential Virtual Machines. The current status of publications is continuously tracked with an internal reporting file.

2.4 Past and planned presentations, conferences, and events

In the first project period, the CONNECT project and its members attended 13 conferences and organized one conference. CONNECT participated in nine workshops and organized an additional four workshops. The CONNECT project also published the first newsletter and two factsheets regarding the use cases. Additionally, CONNECT has initiated an interview series where various partners and individuals are interviewed regarding their roles in the project and their perspectives. In Section 2.5.1 some Highlights are described.

2.4.1 Highlights

Escar Europe 2023, November 15 & 16, 2023

Escar Europe is a premier conference focusing on automotive security which took place for the 21st time on November 15 and 16, 2023. Escar Europe 2023 conference has seen the largest number of participants ever with a total number of 281 in-person participants and 51 online participants. Seventeen conference speakers have covered a wide range of automotive security topics ranging from cryptography, secure development of IT and AI, security management, to system security. Prof. Kargl acted as conference chair. CONNECT project was represented with a talk by Nataša Trkulja from Ulm University on the topic of "In-vehicle Trust Assessment Framework." The talk focused on the work published in a joint paper of the same name between Ulm University, DENSO

AUTOMOTIVE, and Huawei Technologies about the conceptual architecture of the Trust Assessment Framework. The talk lasted twenty-five minutes, with a five-minute-long Q&A session. There were many questions and high interest in the work presented during the Q&A session, as well as afterwards. The speaker was approached by multiple original equipment manufacturer and tier supplier representatives including Daimler Truck, Hyundai Mobis, Garrett Motion, and Cymotive, who all expressed great interest in the work CONNECT is doing.



Figure 2:Nataša Trkulja from Ulm University on the topic of "In-vehicle Trust Assessment Framework."

ETSI Security Conference

CONNECT participated to the ETSI Security Conference, Sophia-Antipolis, 16-19 October 2023. A full report on the CONNECT participation is found in chapter 4.3.3 of the present document.

Newsletter

The first CONNECT newsletter was published in August, which included a message from the coordinator, information about technical meetings, and updates on the consortium. Additionally, there was an update on the technical work done so far in the project per work package, along with information about past interviews and upcoming events.



Figure 3: First CONNECT newsletter:

[LINK](#)

Fact Sheet 1 & 2

The CONNECT project has released two informative fact sheets to elaborate on its initiatives.

[Fact Sheet One](#) addresses Trust Assessment, providing insights into the design of a trust management framework. This framework is pivotal for assessing trust and making informed trust decisions within the context of Cooperative, Connected, and Automated Mobility (CCAM) systems. It emphasizes the necessity of a dynamic and continuous trust evaluation process, incorporating Subjective Logic to manage uncertainties and quantify trust levels effectively.

[Fact Sheet Two](#) delves into the concept of trustworthiness, highlighting the ethical values and characteristics that are essential for ensuring the integrity and reliability of CCAM systems. It underscores the importance of ethical considerations in the development and deployment of these systems, ensuring that they not only meet technical specifications but also align with societal values and norms.

Both fact sheets collectively present a comprehensive view of the CONNECT project's efforts to integrate trust management and ethical considerations into the future of automated mobility, ensuring safer, more reliable, and ethically responsible technological advancements.

Interviews

The Connect project initiated an interview series to provide deeper insights into the roles of various partners within the project. Currently, the project website features four interviews. These include conversations with Frank Kargl, the scientific lead from UULM, and Thanassis Giannetsos, the technical lead from UBITECH, along with two use case partners. Francesca Bassi from IRTSX discusses the "Intersection Movement Assist" use case, and Alexander Kiening from DENSO covers the "Vulnerable Road User Protection" use case. The CONNECT project plans to conduct additional interviews to offer a more comprehensive overview of the project's status and the diverse roles of its partners. Figure 4 shows an example of a produced interview.



Figure 4: Interview Alexander (Denso) [LINK](#)

Technical and Advisory Board meetings

Throughout the development phase of the CONNECT project, a series of technical meetings were conducted to facilitate collaborative problem-solving and ensure alignment with project goals. These meetings served as a platform for team members to present progress updates, discuss technical

challenges, and brainstorm solutions. The collaborative environment fostered by these meetings was instrumental in driving the project forward, ensuring that technical developments were closely aligned with the overarching objectives. On 13 February 2024, the CONNECT project held its first online advisory board meeting with six members of the advisory board joining, leading to insightful discussions. For all meetings brief summaries and updates are available on the CONNECT project website, so that stakeholder can follow the project progress and additionally they are promoted on social media for wider engagement. For example, Figure 5 shows a group picture of the technical meeting in Munich hosted by Denso.

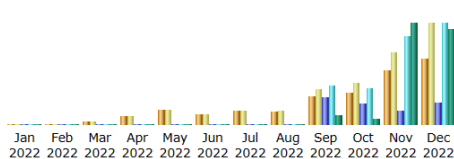


Figure 5: Technical meeting Munich: [LINK](#)

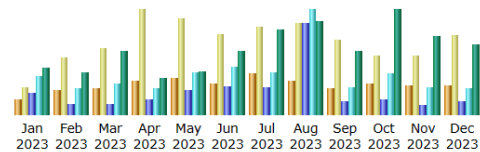
2.5 Project website

The CONNECT website continues to be one of the main dissemination and communication tools for reaching a wide variety of audiences. According to Advanced Web Statistics 7.6 (see figure below), the CONNECT website was visited 69.945 times by 29.160 unique visitors during September 2022 and January 2024. The average visits session duration was 74 seconds.

The website has been so far updated with the most relevant information regarding our results, meetings, as well as past and future events.



Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2022	0	0	0	0	0
Feb 2022	0	0	0	0	0
Mar 2022	17	17	29	29	153.86 KB
Apr 2022	60	61	64	64	438.91 KB
May 2022	112	112	121	121	815.22 KB
Jun 2022	80	81	83	83	588.64 KB
Jul 2022	105	106	116	116	768.05 KB
Aug 2022	98	103	107	107	742.64 KB
Sep 2022	212	261	3,821	5,420	361.91 MB
Oct 2022	238	310	2,861	5,134	238.78 MB
Nov 2022	397	528	2,033	12,538	3.92 GB
Dec 2022	484	739	3,173	14,290	3.74 GB
Total	1,803	2,318	12,408	37,902	8.25 GB



Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2023	1,108	1,963	15,528	28,277	4.66 GB
Feb 2023	1,775	4,143	7,727	18,456	4.14 GB
Mar 2023	1,883	4,853	7,499	22,295	6.23 GB
Apr 2023	2,499	7,543	10,852	18,584	3.57 GB
May 2023	2,623	6,884	18,258	30,088	4.31 GB
Jun 2023	2,255	5,826	20,286	34,744	6.23 GB
Jul 2023	2,964	6,360	19,640	30,229	8.43 GB
Aug 2023	2,452	6,556	65,293	74,894	9.23 GB
Sep 2023	1,874	5,384	9,701	19,699	6.28 GB
Oct 2023	2,202	4,240	11,032	29,155	10.32 GB
Nov 2023	2,168	4,255	7,146	19,296	7.72 GB
Dec 2023	2,130	5,779	9,208	18,387	6.96 GB
Total	25,933	63,786	202,170	344,104	78.07 GB

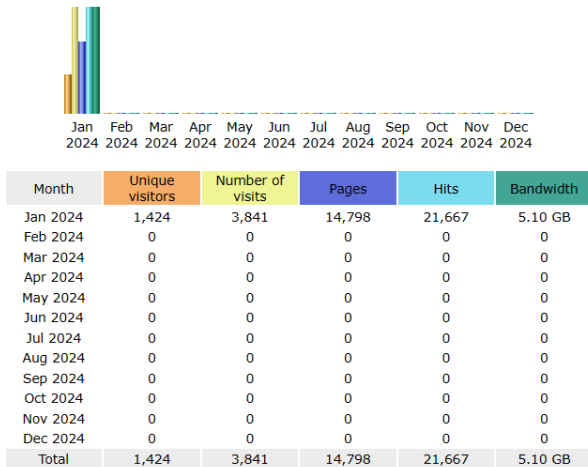


Figure 6: Website statistics CONNECT.

2.5.1 Social media

The CONNECT project’s activities are disseminated on https://twitter.com/connect_horizon. So far, CONNECT has 45 followers and 100 posts. Due to further activities and connections with interested users those numbers are planned to be raised significantly. During the 2nd period the CONNECT X account made more than 1.000 impressions. X counts impressions as the number of times users saw your tweets on X. X provides statistics per months, in Figure 7 below you see an example for October 2023.

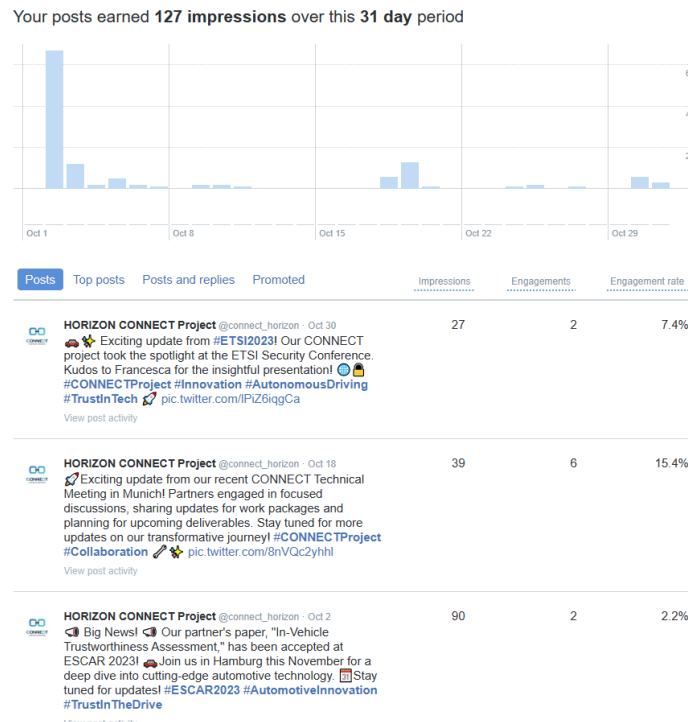


Figure 7: X-Statistics

LinkedIn is a social networking site for people in professional occupations or simply a social network for business. CONNECT can be accessed via: <https://www.linkedin.com/company/horizon-europe-connect-project-101069688/>. So far, the CONNECT project has 137 followers. During the first period the CONNECT LinkedIn account made more than 14.433 impressions. LinkedIn counts impressions as the number of times your content shows up on a screen. Figure 8 shows the impressions of last months (October 2023 to January 2024).

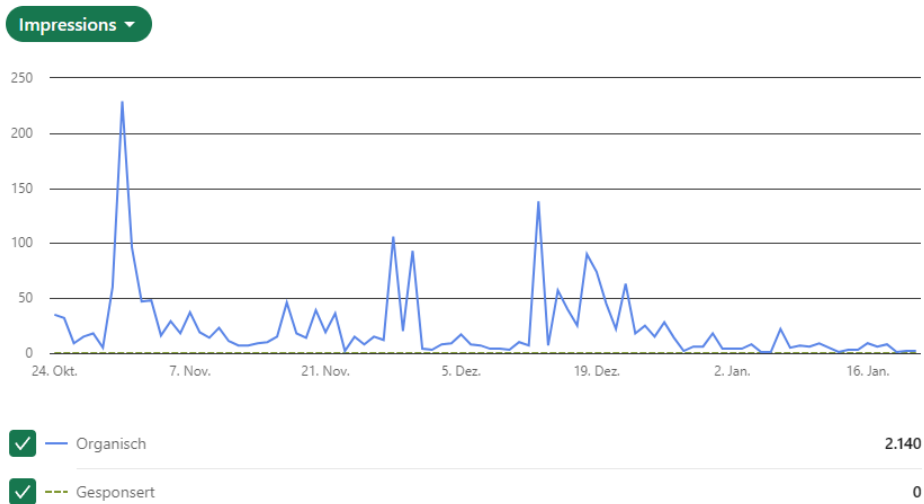


Figure 8: LinkedIn statistics.

Figure 9 shows the statistics per post for LinkedIn, the impressions and likes recorded vary per post and can be higher or lower depending on the topic. Figure 9 shows the average of a CONNECT post with 707 views, 16 reactions and five shared posts.

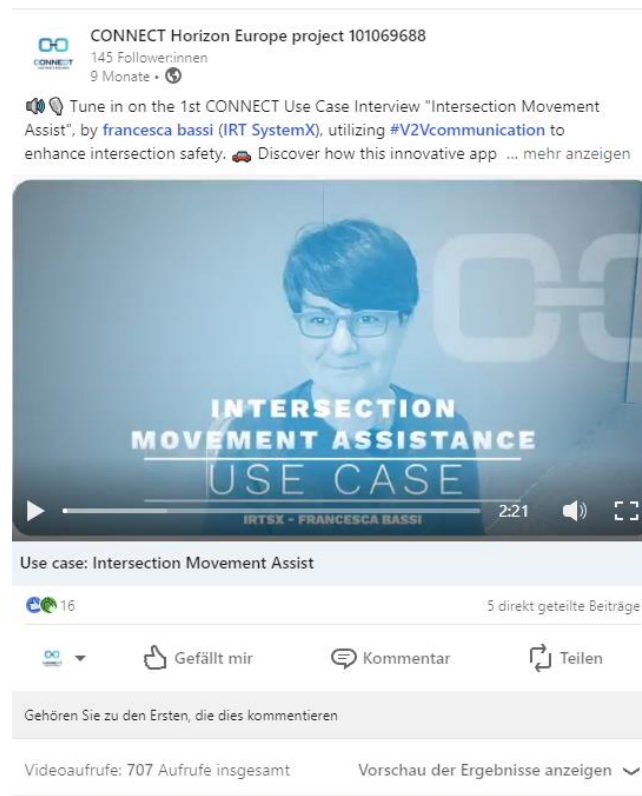


Figure 9: LinkedIn statistics per entry.

Using relevant hashtags, the CONNECT project aims to maximise the audience reached by each post which is published on social media. Both accounts are updated on a regular basis and to schedule the postings and tweets, a posting plan was set up, which helps to plan and organize upcoming content. Direct links to the CONNECT Twitter Account and the LinkedIn page can be also found on the CONNECT website.

Chapter 3 Clustering

3.1 Introduction

Chapter 3 covers the project's active participation in activities organized by clusters/associations relevant to CONNECT results as described for task T7.2. CONNECT partners participated in the 5GAA and CCAM communities with the objective of enabling the acceleration of the CONNECT adoption by the CCAM industry. Activities at AIOTI, the CAR 2 CAR Communication Consortium and data spaces communities further strengthen the establishment of relationships with community stakeholders, such as cybersecurity and automotive vendors who can benefit from CONNECT artefacts to address the existing challenge for secure CCAM services.

3.2 5GAA

The 5G Automotive Association (5GAA, <https://5gaa.org/>) is a global, cross-industry organization of companies from the automotive, technology, and telecommunications industries (ICT), working together to develop end-to-end solutions for future mobility and transportation services. The main essence of 5GAA work is to bring together two main categories of stakeholders: First, telecommunication companies (like operators, neutral hosts, network technology providers, chip makers, etc.) that are providing connectivity and networking systems, devices, and technologies. Second, automotive players (like vehicle OEM manufacturers, OEM suppliers, system integrators, etc.) that work on vehicle platforms, hardware, and software solutions. 5GAA has more than 120 industry members, including automotive manufacturers, tier-1 suppliers, chipset/communication system providers, mobile operators, and infrastructure vendors.

Trust in C-ITS becomes an increasingly important topic in 5GAA. Several WIs have called for the need to establish trust in the use of MEC in C-ITS applications, as well as in the exchange of geolocation information between vehicles and other sensor sharing applications. However, establishing mutual trust has been discussed only in the context of Safety so far, while the discussion on technological innovation for trust only begins now.

Several activities within 5GAA can be considered in synergy with the concept of trust:

- The recent 5GAA study on Cybersecurity for Edge Computing [4] argues that at the moment is not possible to establish mutual trust between MEC applications and MEC platforms, and presents an analysis of the technological gap existing at the moment for achieving trust in such environments for the automotive domain.
- The problem of assessing the trustworthiness of geolocation information is specifically analysed in the recent report [5]. When OEMs receive V2X messages which include positioning information they do not know what level of trust they can associate to the received content and as such they do not know whether the car OEM can exploit the information.
- Another recent report [6] elaborates on mutual trust concept from the safety perspective, underlying security concepts (e.g., similar to the Protection Profile V2X Hardware Security Module currently under discussion in the C2C-CC).
- A 5GAA White Paper on Misbehaviour Detection [7] captures the effort within 5GAA on how to solve the problem of bad actors and/or malfunctioning devices with valid credentials flooding the V2X network with bad and even harmful data. The goal is to use MBD system for making V2X messages more trustworthy.

CONNECT has established a liaison with 5GAA and regularly reports the project results to the 5GAA participants, arguing on the relevance to current activities in the association.

In addition to that, CONNECT partner, Huawei, has initiated and edited a new White Paper that is dedicated in defining the problem of trust establishment for connected and autorotated vehicles. This White Paper communicates the work from D3.1 "Architectural Specification of CONNECT Trust

Assessment Framework, Operation and Interaction" [2] and D2.1 "Operational Landscape, Requirements and Reference Architecture – Initial Version" [1] on the definitions of trustworthiness, the need to have dynamic trust assessment based on verifiable evidence, and the need to build trust assessment framework that can reason with uncertainty.

More specifically, the contribution of CONNECT to the 5GAA White Paper "Creating Trust in Connected and Automated Vehicles" is to explicitly describe how to address the challenge of dynamic trust assessment from the perspective of CONNECT and the work described in D3.1 [2] and D2.1 [1]:

- The document primarily defines the concept of trust and trustworthiness for the vehicle domain.
- It defines the notions of trust network and different types of trust relationships (direct, derived, functional and referral).
- It lists and defines several properties that can be used in the context of connected and automated vehicles.
- It presents a list of potential trust sources from several categories, such as security, safety, etc.
- It hints on the use of Subjective Logic to be able to reason with uncertainty based on evidence, and how this becomes a fundamental approach in trust assessment.

At the moment of writing the present deliverable, the White Paper has been submitted for final endorsement by the 5GAA participants and is expected to be published in the next few months.

3.3 CCAM

Connected, Cooperative & Automated Mobility (CCAM) is discussed in the 2021 established CCAM Association (<https://www.ccam.eu/what-is-ccam/ccam-association/>) with the objective of assessing impacts and understanding user and societal effects to harmonize European R&I efforts to accelerate awareness and implementation of innovative CCAM technologies and services and to exploit the full systemic benefits of new mobility solutions enabled by CCAM: increased safety, reduced environmental impacts, and inclusiveness.

Also in 2021, the CCAM partnership (<https://www.ccam.eu/what-is-ccam/ccam-partnership/>) was established with the objective of creating a more user-centred and inclusive mobility system, increasing road safety while reducing congestion and environmental footprint and of encouraging collaborative research, testing and demonstration projects in order to accelerate the innovation pace and implementation of automated mobility. It is seen as essential to work together at a European level to help remove barriers and to contribute to the acceptance and efficient rollout of automation technologies and services.

3.3.1 CCAM Association

The CCAM Association is an international non-profit organization focused on advancing research in the context of CCAM. The association plays a pivotal role in bringing together various stakeholders in the CCAM value chain, including industry players, research institutions, and public entities. In total the CCAM Association has 214 members, amongst which several partners of the CONNECT project (ICCS, Huawei, DENSO, University of Surrey, and Polytechnic University of Turin). Its main objective is to foster collaboration and coordination of research and innovation activities in the field, both at the European and international levels. The association aims to streamline and harmonize efforts across Europe to accelerate the development and implementation of innovative CCAM technologies and services.

A significant aspect of the CCAM Association's activities involves its connection with the CCAM Partnership. The CCAM Partnership represents a co-programmed partnership with the European Union, as defined by the Regulation establishing the Horizon Europe program. This collaboration signifies a strategic alignment with the European Commission in implementing framework programs

related to research, innovation, and demonstration in the CCAM sector. Through this partnership, the CCAM Association contributes to shaping the European research and innovation landscape in the field of automated mobility, facilitating a cohesive approach towards achieving common goals and addressing shared challenges in this rapidly evolving sector.

The CCAM Association, among others, strengthens the dissemination of CONNECT results among the researchers in the field of CCAM, and as a result, improve the coordination of research efforts in this field in Europe.

3.3.2 CCAM Partnership

European partnerships (in the context of Horizon Europe) are key implementation tools contributing to the realization of the EU's political priorities. Partnerships bring together the European Commission with private and public stakeholders to coordinate research and innovation actions. Along these lines, the CCAM (public private) partnership has been established in 2021 aiming to achieve key policy goals such as the UN Sustainable Development Goals [8] (SDG), the European Green Deal [9] and the Smart and Sustainable Mobility Strategy [10].

Towards that end, more than 200 CCAM stakeholders have become CCAM Partnership members aligning their research efforts to accelerate the implementation of innovative CCAM technologies and services in Europe. The Partnership has introduced a shared, coherent, and long-term R&I agenda/roadmap [11] to materialize the CCAM Partnership strategy. The document introduces the Partnership's objectives and defines the process to support the research and innovation activities required for meeting the identified objectives; the involved resources and timeline are also described. Interestingly, Secure, and trustworthy interaction between CCAM entities has been recognized as a Specific Objective, highlighting the CONNECT relevance.

ICCS, Huawei, DENSO, University of Surrey, and Polytechnic University of Turin are members in the CCAM Association, serving as vehicles to bring the CONNECT vision and results in the attention of the partnership and exercise influence on the development of trustworthy CCAM technologies.

The CCAM Partnership organizes its activities into 7 different clusters. Each cluster focuses on a specific aspect of Connected, Cooperative, and Automated Mobility. Cluster 5, in particular, deals with Key Enabling Technologies integrating the vehicle in the intelligence transportation system. This cluster is critical as it encompasses the foundational technologies that drive advancements in the CCAM field.

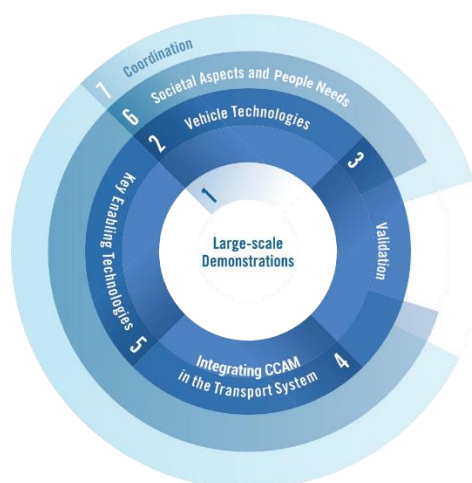


Figure 10: The seven CCAM clusters

CONNECT is an answer to the CCAM Partnership's Work Programme and is thus running under the umbrella of the CCAM Partnership, and more specifically within Cluster 5. This cluster contributes to and benefits from the research, development, and innovation efforts focused on these key

technologies. Cluster 5 is instrumental in fostering technological advancements that underpin the wider objectives of the CCAM Partnership.

More specifically, CONNECT has given input to the CCAM Multicluster meeting, where through several sessions it provided CONNECT's viewpoint and research directions as feedback which was later compiled into the CCAM Partnership's Strategic Research and Innovation Agenda (SRIA) [11].

The following table shows the activities of CONNECT in relation to CCAM Partnership.

Date	Activity type	Activity
23-25 October 2022	CCAM Association Multi-Cluster Meeting, Brussels, Belgium	CONNECT presented its objectives to the plenary as part of Cluster 5 project and gave feedback at the drafting of the new version of the SRIA.
5-7 February 2024	RTR Conference on results from road transport research, Brussels, Belgium	CONNECT invited to present main results and long-term impact as part of Cluster 5 project.

Table 4: CONNECT activities at CCAM Partnership

3.4 CAR 2 CAR Communication Consortium

The CAR 2 CAR Communication Consortium (C2C-CC, <https://www.car-2-car.org/>) is an association of major European automobile manufacturers and suppliers and research institutes. It aims at assisting towards accident-free traffic (vision zero) at the earliest possible date. It further aims at supporting the highest safety level at improved traffic efficiency anywhere, anytime at the lowest cost to the end user and the environment. While working on solutions supporting all driving levels from manual to fully automated it considers specific needs of stakeholders, types of vehicles and users.

The C2C-CC contributes to the development and specification of robust and reliable solutions that allow for a continuous and seamless evolution of required functionalities. It enables technologies driven by innovation and competition, thereby fostering concepts of cooperation between the road users and with the road infrastructure. This is based on sharing information, awareness, perception, and intentions while focusing on tactical level and considering strategic and planning level as required.

IRTSX and UULM are both a member of the C2C-CC. In the recent past, IRTSX has actively participated to a working item on Misbehaviour Detection and Reporting. A resume of the activity within C2C-CC is planned, with the aim of identifying a suitable working group for dissemination activities on CONNECT.

3.5 AIOTI

AIOTI (<https://aioti.eu/>) is the leading Internet of Things organization in the EU. It aims to *lead, promote, bridge, and collaborate in IoT and Edge Computing and other converging technologies research and innovation, standardization, and ecosystem building, providing IoT and Edge Computing deployment for European businesses creating benefits for European society.*

AIOTI runs vertical working groups (agriculture, energy, health, manufacturing, mobility) as well as horizontal working groups (research and innovation, standardization, testbeds, policy, ICT for CO₂ reduction methodologies).

AIOTI is particularly active in standardization through liaisons with ISO/IEC JTC1/SC41 (IoT and Digital twins) and ITU-T SG20 (Internet of things (IoT) and smart cities and communities (SC&C) Internet of things (IoT) and smart cities and communities (SC&C))

AIOTI standardization WG includes several activities of interest to CONNECT:

- High-level architectures and digital twins.
 - AIOTI is currently leading the preparation of white paper on digital twin contributions from European research projects. This paper, jointly authored by AIOTI, BDVA/Adrae, StandICT and HS Booster will be submitted to ISO/IEC JTC1/SC41 and is relevant to CONNECT activities on digital twins.
 - AIOTI will be working jointly with the EUCloudEdgeIot (<https://eucloudedgeiot.eu/>) project on a computing continuum architecture document that will be submitted to ISO/IEC JTC1/SC41.
- Security and privacy
- Semantic interoperability

AIOTI is an instrument for clustering activities. CONNECT project partners TRIALOG, FSCOM, HUAWEI are active members.

3.6 Data spaces community

3.6.1 General

The EU Data Strategy is a key component of the Digital Europe Program. It aims to unlock the potential of data for the benefit of the European economy and society. The strategy focuses on facilitating data sharing and data-driven innovation while respecting privacy and security. It promotes the creation of common European data spaces in various sectors, including healthcare, agriculture, and mobility.

The European Mobility Data Space (EMDS) is part of the EU Data Strategy and focuses specifically on the mobility sector. It aims to create a framework for the sharing and use of mobility data to improve transportation services, reduce congestion, and enhance sustainability. This initiative seeks to enable the seamless exchange of data between various stakeholders, such as transportation companies, public authorities, and researchers, to foster innovation and improve mobility across Europe.

In general Mobility Data Spaces is a relatively new concept in the field of mobility and data management. It refers to a platform that enables the sharing and exchange of data related to mobility among various stakeholders in a secure and controlled way. Mobility Data Spaces can be seen as a data ecosystem that brings together data producers and data consumers, enabling them to create value from data and generate new business opportunities. At the moment there are several initiatives that focus on promoting the convergence of various other data spaces, such as logistics and manufacturing.

3.6.2 PrepDSpace4Mobility

Serving as a preparatory action, PrepDSpace4Mobility is dedicated to laying the foundational groundwork for the development of the common European Mobility Data Space (EMDS). This initiative is key in identifying existing data ecosystems and proposing comprehensive frameworks for data exchange and management within EMDS.

In that way, PrepDSpace4Mobility's role in preparing the groundwork for EMDS is invaluable, ensuring that the future EMDS is built on a solid technical foundation. This involves leveraging existing EU reference architectures and federated data sharing models from initiatives like the International Data Spaces Association (IDSA), Gaia-X, and iSHARE. By integrating these existing models, the report suggests a harmonized approach to developing a robust reference architecture for EMDS. This architecture would facilitate secure and efficient data sharing and management across various mobility and logistics stakeholders in Europe. The focus is on ensuring that the technical infrastructure supports interoperability, scalability, and flexibility, allowing for the integration of a wide range of data sources and types within the mobility ecosystem.

Data sovereignty and trust are identified as pivotal aspects of the EMDS. In its recent report, PrepDSpace4Mobility highlights the importance of adopting decentralized trust mechanisms and

robust consent management systems, which are crucial for maintaining data sovereignty [6]. Trust is built by implementing mechanisms that guarantee the integrity and confidentiality of data, and by providing transparency in data processing and sharing practices. The report suggests that establishing these frameworks for data sovereignty and trust is essential for encouraging stakeholder participation and for the overall success of the EMDS.

These points highlight the critical role that CONNECT plays in establishing a trust framework for data sovereignty and encouraging stakeholder participation in EMDS. CONNECT being the only trust assessment framework that is tailored to the requirements of dynamic data (such as mobility data) is key to overcoming challenges related to data sharing and trust among various stakeholders in the European mobility data ecosystem.

3.6.3 IDSA

The International Data Spaces Association (IDSA) is involved in the development and standardization of data spaces, including mobility data spaces. More specifically, the Mobility Data Spaces is built on the IDSA's Reference Architecture Model (RAM), in order to establish an ecosystem in which data providers can specify and control the conditions under which others utilize their data. This enables data sovereignty and trust, providing users with assurance regarding data origin and quality. By integrating open and private data through IDS-based data connectors, the MDS becomes a digital distribution channel for data-driven business models.

CONNECT's partner, Huawei, is actively involved in the Architecture WG of IDSA producing the IDSA RAMv5, conveying a lot of ideas of CONNECT on dynamic trust assessment. One of the goals of IDSA RAM is to ensure the quality and reliability of data. In the mobility sector, trust assessment includes validating the accuracy, completeness, and integrity of mobility data. As the RAM architecture moves to more decentralized models, CONNECT's artifacts on dynamic and distributed trust assessment fit perfectly in this direction.

In addition, Huawei has joined the recently established standards coordination group of IDSA.

3.6.4 FAME

The FAME [12] EU research project (gathering 22 partners coming from 12 EU member states) seeks to introduce and validate a harmonized CCAM test framework for vehicle automation capabilities on European roads. Along this line, the involved automotive data exchange needs to rely on common features (e.g., data formats etc.) and processing (e.g., annotation, legislation-compliance etc.) procedures. One of the project's relevant contributions (towards the establishment of the framework) is the development of a CCAM test data space, mainly through applying test data sharing best-practices over an existing platform (realising the Gaia-X specifications).

The expected FAME data space will support data exchange relying on trust and data sovereignty. The concept will draw on the Gaia-X concepts and ensure further interoperability by employing common formats and annotation models for data of different stakeholders. FAME will use an existing data space platform and define initial use cases to highlight the best practices on data protection, data description (e.g., formats, test metadata) and legal agreements between actors. A CCAM data catalogue and relevant management tools will be also developed. The FAME data space use cases will cover the data transfer from data provider to data consumer as well as the data provider processing tasks (at its own infrastructure) and the results sharing with a consumer.

Clearly, the considered CCAM space can only become a reality when the sharing involves trusted data between the CCAM community stakeholders. The involved trust assessment needs point directly to the CONNECT contributions and suggest yet another application domain for the CONNECT research. Communication (and potential liaison) links to the FAME achievements will be established through ICCS which participates in both consortia.

3.6.5 GAIA-X

GAIA-X is an initiative aimed at creating a secure, federated system that fosters the digital sovereignty of Europe. It establishes common standards for data infrastructure and services, ensuring that data is stored and processed in ways that comply with European values and regulations, thus promoting transparency, openness, and trust in digital ecosystems.

In the mobility domain, the Mobility Data Space will constitute the Data Ecosystem layer within the Gaia-X architecture and will also comprise Advanced Smart Services, e.g., employing artificial intelligence fuelled by the data, thus providing the foundation for new disruptive applications. Furthermore, the Mobility Data Space Services will be made interoperable with the Gaia-X Federation Services.

In this challenging environment where each Data Space wants to both be interoperable and yet adapts their governance to their vertical, domain-specific needs, local market regulation, the Gaia-X Trust Framework provides a set of world-wide applicable rules and specifications usable by the ecosystem governance (e.g.: Data Spaces authorities, such as Data Intermediaries from the Data Governance Act) and also for ecosystems seeking interoperability and technical compatibility of their services.

The ecosystem governance defines the applicable policy rules to participate in the digital (infrastructure, data, or services) ecosystem, together with the Trust Anchors and Schema Extensions policy rules which apply to operators of services in the specific ecosystem. Trust Anchors are entities endorsed by Gaia-X. Trust Anchors shall underpin claims by Participants. Consequently, Trust Anchors shall facilitate the processing of claims by Participants as Trust Anchors will - subject to their fair and transparent procedures - affirm the necessary trust in otherwise mere self-declared statements.

CONNECT integrates trusted computing capabilities (Roots of Trust) in the vehicles to create a “Network of Trust” and produce self-declared statements as claims on the trustworthiness of the data produced by vehicles. CONNECT is aiming to align this with the GAIA-X trust framework, through CONNECT’s partner, Huawei. More specifically, Prof. Theo Dimitrakos is a voting member of Gaia-X Architecture WG and new Policy Rules Committee (PRC) working group.

Chapter 4 Standardization

4.1 Introduction

Chapter 4 covers the project's active participation in standardization activities relevant to CONNECT results as described for task T7.3. CONNECT partners ensure that CONNECT is in line with relevant global standards and legislations and identify appropriate sections of research that are brought into the standardization and liaison process, leveraging dialogues with relevant bodies to share findings and innovations. In the first half of the project's lifetime, standardization activities focused on ISO TC204 and JTC1 and the ETSI groups TC ITS and ISG MEC.

4.2 Contribution to ISO

4.2.1 TC204 (Intelligent Transport Systems)

ISO Technical Committee 204 on 'Intelligent Transport Systems' has recognized that Artificial Intelligence and Big Data standardization is gaining momentum in all different domains of standardization. Consequently, WG20 on 'Big Data and Artificial Intelligence supporting ITS' has been established to work on ITS specific use cases in this field. WG20 had its first meeting in April 2022 and shortly after has launched a call for contribution to obtain appropriate ITS specific and AI and/or Big Data relevant inputs, namely specific use cases that take advantage of big data and artificial intelligence. for this standardization work. Collected inputs will be published in the ISO technical report TR 12786 titled "Intelligent transport systems — Big data and artificial intelligence supporting intelligent transport systems — Use cases".

CONNECT representatives that closely follow the ISO TC204 proceedings have distributed the call for input amongst the project partners. The below use case has been selected and then contributed on 1 October 2022 to WG20.

Name of the use case	Edge Misbehaviour Detection for V2X data reliability
Objectives	ITS stations produce reports about semantic inconsistencies in received V2X messages, destined to an edge backend entity (edge cloud) which uses AI in order to determine the dependability of the stations with respect to the transmission of data and disseminate the result. The objective is to strengthen the reliability of the semantics of V2X messages, which is essential to the operation of autonomous vehicles.
Stakeholders	ITS ecosystem, edge cloud operators.
Short description	The ITS system is prone to insider attacks by legitimate stations that may divulge inaccurate data (either unintentionally or maliciously). Edge Misbehaviour Detection aims to detect attackers and to alert stations in real-time, so that they can consume received V2X data appropriately. The system is composed of a Local Misbehaviour Detection function embedded in the nodes, which produces reports on the received data; and of an Edge Misbehaviour Detection function, which collects and processes the reports at the edge. The edge component leverages AI algorithms to determine the dependability of the stations and disseminates the results to the stations.
Technical description	The system is composed of two components. The Local

	<p>Misbehaviour Detection function is embedded in the receiving station (vehicle, roadside equipment, nomadic device). The Local Misbehaviour Detection function parses all received data in order to identify inconsistencies within the message, or between multiple messages received by the same or by distinct sources. As soon as these inconsistencies are detected, the Local Misbehaviour Detection function produces reports and offloads them to the edge component. The reports need to contain the messages deemed inconsistent. The Edge Misbehaviour Detection function collects all the reports that are generated in the geographical area. These data are processed by AI algorithms which aim to identify the nodes whose data is not to be considered fully trustworthy, and possibly to quantify the trustworthiness penalty that those stations should incur. The Edge Misbehaviour Detection function then produces alerts about untrustworthy stations that are broadcasted in the reference geographical area. Stations employ the alerts generated by the Edge Misbehaviour Detection component to decide how to consume the received V2X data in their driving functions.</p>
Data characteristics	<p>Reports form the stations to the edge: they contain the received messages deemed inconsistent by the Local Misbehaviour Detection component.</p>
Challenges	<p>The main challenge is that in order to be effective, the system needs to be able to correctly identify untrustworthy stations in a very short amount of time. This requires very small latencies for both the Local Misbehaviour Detection and the Edge Misbehaviour Detection functions.</p> <p>The efficiency of the system in detecting stations emitting untrustworthy data might be partially compromised by policies mandating too frequent changes of pseudonym signatures.</p> <p>A further challenge is represented by the possible breach in privacy coming from the offloading of data, in the form of reports, from the stations to the edge.</p>

Table 5: CONNECT input to ISO TR12786

To illustrate the necessary workload of just promoting the inclusion of a single project use case into a technical report, the following table shows the ISO TC204 WG20 activities in which project representatives participated in relation to the CONNECT use case contribution to ISO TR12786.

Date	Activity type	Activity
05/10/2022	WG20 F2F during 60 th ISO TC204 plenary in Tampere	Review of first UC contributions including CONNECT UC.
31/10/2022	-	Closure of UC submission, CONNECT UC accepted.
22/12/2022	WG20 activity call	Review of document with focus on UCs.
26/01/2023	WG20 activity call	Review of document with focus on UCs.
28/02/2023	WG20 activity call	Review of document with focus on UCs.
30/03/2023	WG20 activity call	Review of document with focus on UCs.

20/04/2023	WG20 activity call	Decision to send ISO TR12786 on WG20 consultation review (22/04 – 11/05/2023).
17/05/2023	WG20 F2F during 61 st ISO TC204 plenary in San Antonio	Start of consultation review comment resolution. 68 comments have been raised.
09/06/2023	WG20 activity call	Continuation of review comment resolution.
29/06/2023	WG20 activity call	Continuation of review comment resolution. No CONNECT participation.
13/07/2023	WG20 activity call	Continuation of review comment resolution.
20/07/2023	WG20 activity call	End of review comment resolution. Decision to send ISO TR12786 on CD ballot (02/08 – 27/09/2023).
25/10/2023	WG20 F2F during 62 nd ISO TC204 plenary in Singapore	Start of CD ballot comment resolution. 19 comments have been raised. No CONNECT participation.
16/11/2023	WG20 activity call	Continuation of CD ballot comment resolution. No CONNECT participation.
29/11/2023	WG20 activity call	End of CD ballot comment resolution.
xx/02/2024	ISO secretariat action	Start of DTR ballot (xx/02/2024 – xx/xx/2024). Exact dates to be defined.
...		DTR ballot comment resolution.
08-12/04/24	WG20 F2F during 63 rd ISO TC204 plenary in Oslo	Next F2F meeting of WG20.
15/07/2024	-	Provisional date for TR publication

Table 6: ISO TR12786 related standardization activities

4.2.2 JTC1 SC27 (Cybersecurity and privacy)

ISO/IEC JTC1 SC27 on cybersecurity and privacy has started several projects of interest in which project partner TRIALOG is involved:

- ISO/IEC 27115 (cybersecurity evaluation of complex system) [14]. The development of this standard started at the end of 2023. It takes an architecture approach to address the evaluation of complex system. It includes both complex systems and systems of systems. The editors of 27115 participate to the CONNECT projects and have studied previously the use case of V2X. It is planned to use the resulting CONNECT architecture as a potential example
- ISO/IEC 27568 (security and privacy of digital twins) [15]. This is a preliminary work item which is building an understanding of the needs on security and privacy in digital twin standards, which will lead to the development of a related standard. It is currently studying use cases (law enforcement, vehicle GPS, conduct of examination, connected vehicle, UAS to assist agriculture digital twin, critical infrastructure using SCADA, Tracking mobile objects

in railways, remote robotic assisted surgery case, consent management case). CONNECT provided the connected vehicle use case.

- ISO/IEC 27090 (Guidance for addressing security threats and failures in artificial intelligence systems) [16] and ISO/IEC 27091 (AI privacy protection) [17]. The development of those two standards started in 2022 and 2023, respectively. Since a CCAM infrastructure can contain AI capabilities, CONNECT will monitor their development and identify items to reuse or to contribute.

In addition, project partner SURREY (University of Surrey) is involved in ISO/IEC JTC1 SC27 WG2 activities. This WG works on the standardization of cryptographic mechanisms. Currently, Professor Chen is serving as a co-editor for the following three projects listed below and also serves as the deputy chairperson of Technical Subcommittee 2 of BSI IST/33, dealing with cryptographic mechanisms and providing input to ISO/IEC JTC1/SC27:

- ISO/IEC 20008-3 Information technology – Security techniques – Anonymous digital signatures – Part 3: Mechanisms using multiple public keys
- ISO/IEC 18014-1:2008 Information technology – Security techniques – Time-stamping services – Part 1: General – Amendment 1
- ISO/IEC 18014-1:2008 Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens – Technical Corrigendum

While this WG and the specifications are not directly focussed on vehicle technology they still do provide valuable input to the work on CONNECT and ideas/results from CONNECT may be fed back into the standards of ISO/IEC JTC1 SC27.

4.2.3 JTC1 SC41 (IoT and Digital Twins)

Project partner TRIALOG is involved in ISO/IEC JTC1 SC41 on IoT and digital twin on several projects of interest:

- ISO/IEC 30188 (Digital twin reference architecture) [18]. The development of this standard started at the end of 2023. It is a horizontal standard that will ensure the interplay with vertical standards in the domain (e.g. smart manufacturing, smart grids, health, agriculture). The standard includes considerations on foundational aspects which have benefited to and from the CONNECT work on architecture in D2.1
 - section 3.4 (Towards Trustworthiness Profiles for CCAM Ecosystems) is based on ISO/IEC/IEEE 42010 [19] and on the orientations taken by ISO/IEC 30188 [18].
 - section 6.8 (Digital Twin for Functional Offloading) study has influenced the specification of the foundational view of ISO/IEC 30188 [18].
- ISO/IEC PWI-17 Guidelines for the integration of IoT and digital twin in data spaces. This is a preliminary work item that is building an understanding of the needs for integration, which will lead to the development of a related standard (a new work item proposal has been submitted). It is expected that the insight provided by the CONNECT use cases will allow for contributions
- ISO/IEC 30149 (IoT Trustworthiness principles) [20] and ISO/IEC 30141 (IoT reference architecture) [21]. These two standard projects are close to publication. The possible impact of those two standards on the technical work of CONNECT will be monitored

Further, AIOTI is preparing with EUCloudEdgelot a contribution on a computing continuum taxonomy that may lead to a preliminary work item. It is planned to present this work item at the next SC41 Plenary (May 2024). Further, ISO/IEC JTC1/SC41 has launched a process to develop ISO/IEC 20123-5 (IoT Behavioural and Policy Interoperability). In the case the development of this standard is accepted, insight provided by CONNECT will be used in terms of interoperability use cases.

4.3 Contributions to ETSI

4.3.1 TC ITS (Intelligent Transport Systems)

Within ETSI TC ITS, which is concerned with the creation of standards enabling the deployment of intelligent transportation systems, the activities of WG5 focus on the security and privacy aspects related to the exchange of information between entities.

ETSI TC ITS WG5 has published several technical specifications that collectively establish the current framework for secure and trustworthy communication among vehicles and infrastructure components. The technical specification ETSI TS 102 940 [22], in particular, specifies the ITS communications security architecture and management. In this context, Misbehaviour Detection is introduced as the functionality that performs checks on the incoming V2X messages; the Misbehaviour Authority is a remote entity able to process Misbehaviour Reports sent by the stations, with the aim of identifying stations that are sending incorrect data.

The technical specification ETSI TS 103 759 [23] introduces the Misbehaviour Reporting Service, which allows a station to produce and send Misbehaviour Reports to the Misbehaviour Authority. The scope of this document is the specification of the format of the Misbehaviour Report and of the dissemination protocol. Moreover, it contains the specification of some misbehaviour detectors.

The Misbehaviour Reporting Service is of interest for CONNECT in the context of the IMA use case, where Misbehaviour Reports are used as a trust source by the TAF. A CONNECT representative is the current *rapporteur* for ETSI TS 103 759 [23]. The ongoing working item targets the specification of the dissemination protocol. The CONNECT scenario has been presented during ITS TC WG5 meeting #68 (June 2023) and is currently considered as a motivating use case. For this occasion, the WG5 chair invited CONNECT to keep liaison activities with TC ITS concerning potential contribution and impact on standardization activities.

4.3.2 ISG MEC (Multi-access Edge Computing)

The purpose of the ISG MEC is to produce deployable Group Specifications, Group Reports, and other collateral (e.g., serialized API specifications, test scripts, API sandboxes, white papers) that enable the hosting of third-party applications in a multi-vendor and multi-operator Multi-access Edge Computing (MEC) environments. ISG MEC coordinates experimentation and showcasing of MEC solutions (e.g., PoCs, MEC deployment trials), and envisages to produce case studies and documents/reports of PoC and trial results. A goal of ETSI MEC is to incorporate operational and delivery experience from the ETSI MEC PoCs and deployment trials and re-introduce concepts into existing and future MEC specifications. This work is considered relevant to the trials performed in the CONNECT deployments.

FSCOM is active in ISG MEC, mainly in the development of test specification and the implementation of APIs and the MEC sandbox which is an interactive environment that enables users to learn and experiment with ETSI MEC Service APIs. These standardized RESTful APIs are targeted towards MEC application developers to expose the value-added services offered by MEC, including real time access to network and context information, as well as location awareness. The design principles for

developing the APIs have also been specified in ETSI GS MEC 009 [24], along with http methods, templates, conventions, and patterns. The MEC service APIs are available in YAML and JSON format at <https://forge.etsi.org>, presented via OpenAPI compliant descriptions.

FSCOM has been involved in several of the Specialized Task Forces (STF) and Testing Task Forces (TTF) that performed the developments of the MEC Sandbox and the testing of the APIs.

- STF569: MEC API Conformance Test Specifications
- STF625: MEC Sandbox Feature Enhancement, Maintenance, and User Support
- STF678: Edge Native Connector: Critical cross-organization MEC Sandbox enhancements
- TTF T012: Maintenance and development of MEC APIs conformance test suites
- TTF T027: Maintenance and development of MEC APIs conformance test suites (follow-up on T012)

4.3.3 ETSI security conference 2023

CONNECT participated to the ETSI Security Conference, Sophia-Antipolis, 16-19 October 2023¹. CONNECT presented a poster contribution, titled *Continuous and Efficient Cooperative Trust Management for Resilient CCAM*, as well as a talk titled *Road-Map Towards the Adoption of Dynamic Trust Assurances for Safety and Security Convergence in Safety-Critical Systems* [25]. Both contributions aimed to introduce CONNECT.

The target problem of trust establishment in CCAM has been presented through examples leveraging the CONNECT use cases, and the general principles of the solutions proposed by CONNECT have been illustrated.

The contribution resonated well with the audience, with a positive reception of the general principles. In particular, the approach proposed by CONNECT has been praised as especially innovative with a participant stating: “This was the most innovative approach of the whole week.”

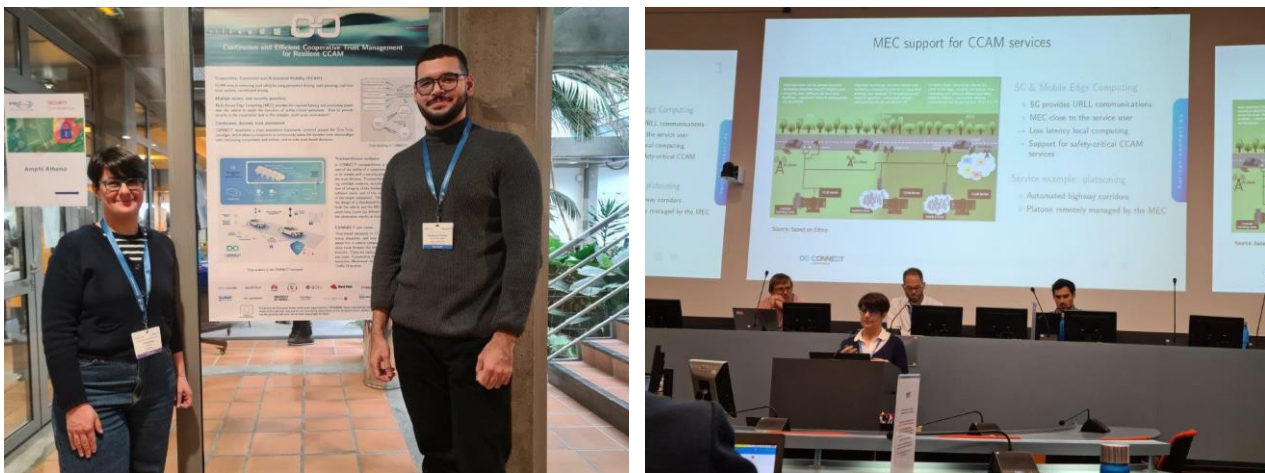


Figure 11: CONNECT presence at ETSI Security conference

¹ <https://www.etsi.org/events/2155-etsi-security-conference-2023>



Cooperative, Connected and Automated Mobility (CCAM)

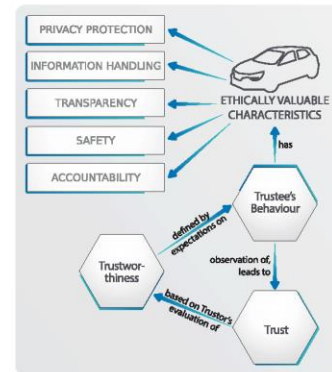
CCAM aims at enhancing road safety by using perception sharing, path planning, real-time local updates, coordinated driving.

Multiple actors, new security questions

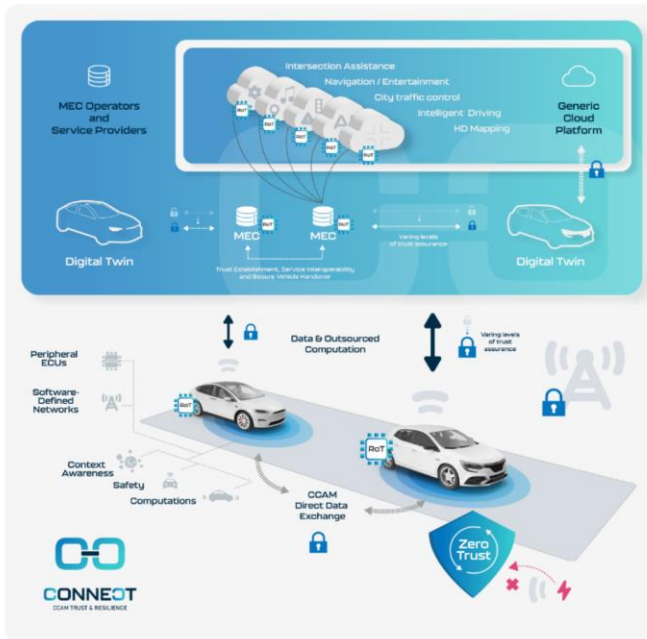
Multi-Access Edge Computing (MEC) provides the required latency and processing power near the vehicle to assist the execution of safety-critical operations. How to provide security in the cooperative task in this complex, multi-actor environment?

Continuous, dynamic trust assessment

CONNECT establishes a trust assessment framework, centered around the Zero-Trust paradigm, which allows a component to continuously assess the dynamic trust relationships with interacting components and entities, and to take trust-based decisions.



Trust modeling in CONNECT



Trust enablers in the CONNECT framework

Trustworthiness evidence

In CONNECT trustworthiness is the technical measure of the ability of a component to perform a task or to comply with a security property, and it informs the trust decision. Trustworthiness is gauged collecting verifiable evidence, including continuous verification of integrity of the hardware, of the instantiated software stack, and of the runtime execution state of the target component. This is obtained thanks to the design of a distributed Root of Trust supporting both the vehicle and the MEC and leveraging trustworthiness claims (as defined by IETF) for disclosing the attestation results as trust sources.

CONNECT use cases

Trust-based decisions in CCAM arise in heterogeneous situations, and may concern, e.g., trust between the in-vehicle components; trust on the V2X data; trust between the vehicle and the MEC infrastructure. These are explored by the three CONNECT use cases: Cooperative Adaptive Cruise Control, Intersection Movement Assistance and Slow Moving Traffic Detection.

Funded by the European Union under grant agreement no. 101069688. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Figure 12: CONNECT poster at ETSI Security conference

4.3.4 ETSI IoT conference 2023

Project partner TRIALOG participated to the ETSI IoT conference, Sophia-Antipolis, 4-6 July 2023² and made a presentation on current activities on digital twins [26].

4.4 Trusted Computing Group (TCG)

CONNECT has also established a liaison with Trusted Computing Group (TCG) which is the internationally accepted standardization group setting all relevant technologies and standards for Trusted Computing (TC) and relevant assurance and attestation schemes. The CONNECT project partners UBITECH and SURREY are members of TCG and regularly participate in the meetings of the TPM Automotive Working Group that focuses on how decentralized Roots-of-Trust (as the ones also leveraged in CONNECT including Gramine Trusted Execution Environment) can provide security benefits to the information technology systems in a vehicle.

UBITECH participated to the TCG (members-only) physical meeting that took place 25 - 29 June 2023 in Berlin, Germany where it presented the latest work of CONNECT towards the provision of secure and certifiable assurance mechanisms for enabling the dynamic trust assessment of in-vehicle E/E topologies by providing integrity guarantees on in-vehicle ECU nodes configurational and behavioural properties as trustworthiness evidence. Such properties, presented as verifiable security claims, are continuously monitored through a harmonized set of TEE Device Interfaces each linked to a separate runtime monitor for capturing the respective state transitions. This allows for the continuous reasoning over any change in the trust level of the monitored assets which, in turn, can trigger the dynamic deployment of additional mitigation measures (e.g., migration of a CCAM function to a neighbouring ECU demonstrating an Actual trust Level – ATL that exceed the Required Trust Level - RTL).

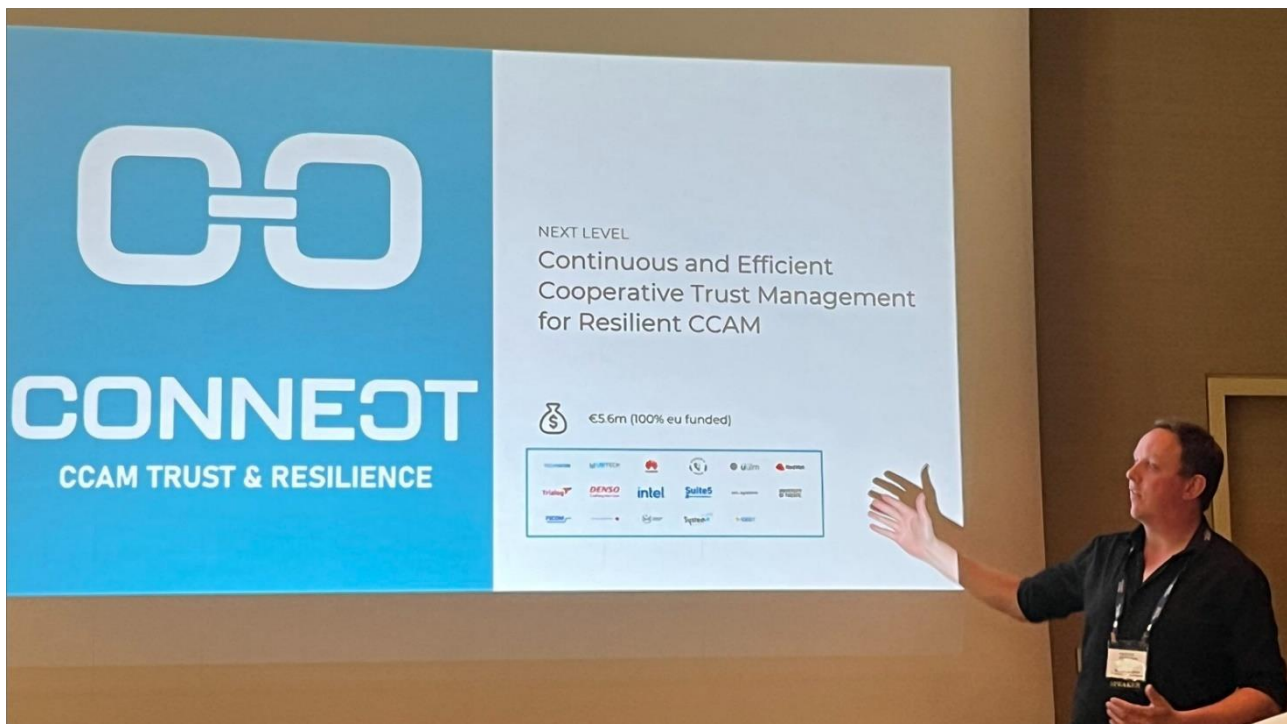


Figure 13: CONNECT presence at TCG Members Physical Meeting in June 2023

In this context, UBITECH is actively contributing to the (currently discussed) specifications of an automotive thin profile that will incorporate such strong integrity guarantees provided by Roots-of-

² <https://www.etsi.org/events/2208-etsi-iot-conference-2023>

Trust embedded into the vehicle. This activity includes the work done in CONNECT in the provision of a novel set of zero-knowledge attestation mechanisms that allow the verification of the configuration state of a node without the need to disclose any sensitive configuration details. This new concept of local attestation enhanced with Verifiable Key Restriction Usage Policies was presented at TCG as an additional functionality to be added in the Trusted Software Stack (TSS). This activity also put forth a fix to a bug (hash loop) that was identified in the TSS. More specifically, there was an issue that impacted the policies- and sessions-related core TPM services and was affecting how these services were managed for enabling the communication with the attached host. Such policies were also implemented in the context of CONNECT's Trusted Execution Architecture. This problem consisted of an infinite hash loop and was solved during the definition and development of the CONNECT Enhanced Configuration Integrity Verification (CIV) protocol by updating the internal functionalities of some TPM commands and building blocks. This elegant solution did not require any modifications or updates to the specification of the existing TPM commands, which would have limited the applicability of the new approach. UBITECH worked together with TCG (more specifically TCG Chair of the TSS stack – Kenneth Goldman) to highlight the issue and propose its fix, which was included in the updated TSS Specification and Implementation as published in the core TCG Github ("Avoiding hash Loops when Making Policies for a TPM 2.0" - <https://github.com/TrustedComputingGroup/TPM/wiki>).

Chapter 5 Open-source Contributions

Besides dissemination and standardization activities, another important aspect of CONNECT's activities pertains to the exploitation opportunities of the various technical artefacts and security enablers to be designed and implemented. The main objective of an efficient exploitation strategy is to ensure that the results and benefits of the developed project outputs are attractive and well-known in the industry. As described in D7.1 [3], CONNECT is committed to an open-source exploitation plan where the core of its innovations and technical artefacts will be published under open-source licensing. In the following, we put forth the first set of information (as discussed by the consortium) for the better understanding of the specific needs of the CONNECT framework as a whole – this is a prerequisite for better practicing open-source approaches especially for such a complex system as the one envisioned in CONNECT comprising a multi-tier set of technical components. It is the first complete Open-Source Development (OSD) plan coping with the CONNECT framework in its entirety setting the scene for the latter separate OSDs to be constructed per CONNECT exploitable asset throughout the remainder of the project and as the implementation activities become more mature. Such exploitable assets revolved around the core innovations of CONNECT on CCAM-wide Trust Assessment, Risk Assessment, Attestation Enablers, Crypto Agility Layer, and Misbehaviour Detection schemes.

The goal is to be able to converge on a common (open-source) exploitation plan and avail for the guidance and support to be provided from ECLIPSE, as part of the OpenContinuum project, ensuring the selection of the optimal exploitation strategy that meets the needs of all stakeholders involved in the project. The CONNECT partner TRIALOG is working on this OSD with ECLIPSE and is already scheduled to provide support to CONNECT in the process towards creating a more detailed breakdown of the plan based on the nature of the technical implementation activities to be finalized by M18 – as the first milestone with the release of the 1st version of the CONNECT overarching framework. This process will culminate with the final OSD fully documented as part of D7.3 with the completion of the implementation and evaluation activities of the final version of the CONNECT framework.

The support will consist of:

- A dedicated online session for explaining the construction of the following CONNECT OSD so as to get concrete feedback based on the envisioned implementation activities.
- Identification of all exploitable assets and the specific needs for the set of CONNECT partners leading their respective implementation and evaluation. This will set the scene for the convergence of a commonly identified license to be adopted for all individual CONNECT exploitable assets.
- Up to four supporting sessions for fleshing out the more detailed OSD break down per asset.

1 Open-source plan info	
Authors name and e-mail	Thanassis Giannetsos (agiannetsos@ubitech.eu) Antonio Kung (Antonio.kung@trialog.com) Ioannis Krontiris (ioannis.krontiris@huawei.com) Guillaume Mockly (guillaume.mockly@trialog.com) Estibaliz Arzoz Fernández (estibaliz.arzoz-fernandez@trialog.com)
History	This constitutes the first version of the CONNECT OSD for the overarching Trust Assessment framework in its entirety. This plan will be enhanced and broken down into separate development plans per exploitable artefact: Trust Assessment Framework, Risk Assessment Engine, Attestation Enablers, Cryptographic Primitives, Runtime Tracer, Misbehaviour

	Detection	
	Date	January 2024
	Version	V0.1
	Description of modification	N/A
Confidentiality	Confidential at consortium and EC level (needed for deliverable)	

Table 7: CONNECT open-source project plan - open-source plan info

2	Context	
Initial Key exploitation result name	CONNECT Trust Assessment Controls – capturing all CCAM-continuum wide trust quantification mechanisms, anchored to Decentralized Roots-of-Trust	
Initial description	Full set of mechanisms, as part of an extensible and programmable framework, for allowing the convergence of security and safety in CCAM by assessing dynamic trust relationships and defining a trust model and trust reasoning framework based on which all involved entities can establish trust for cooperatively executing safety-critical functions.	
Key exploitation result name	CONNECT Trust Assessment Controls	
Description	All components and schemes designed will be agnostic to any specific trusted computing technologies so as to not hinder the applicability of the overall solution. However, the first concrete implementation will be based on the Gramine Trusted Execution Environment (TEE), as the underlying security enabler, for allowing the integration and evaluation of all provided security services in the context of the envisioned use cases. Gramine technology was adopted as one of the most prominent TEE solutions that is efficient enough to not intervene with the operational profile of the target embedded devices. Furthermore, this is the technology offered by the CONNECT INTEL partner. Finally, this allows the harmonization of CONNECT’s trusted software stack across the entire CCAM continuum, including also the MEC, where the enclave-CC will be leveraged based on the use of Gramine as the underlying trust anchor. There are already integration points fleshed out as part of the overall CONNECT integration activities.	

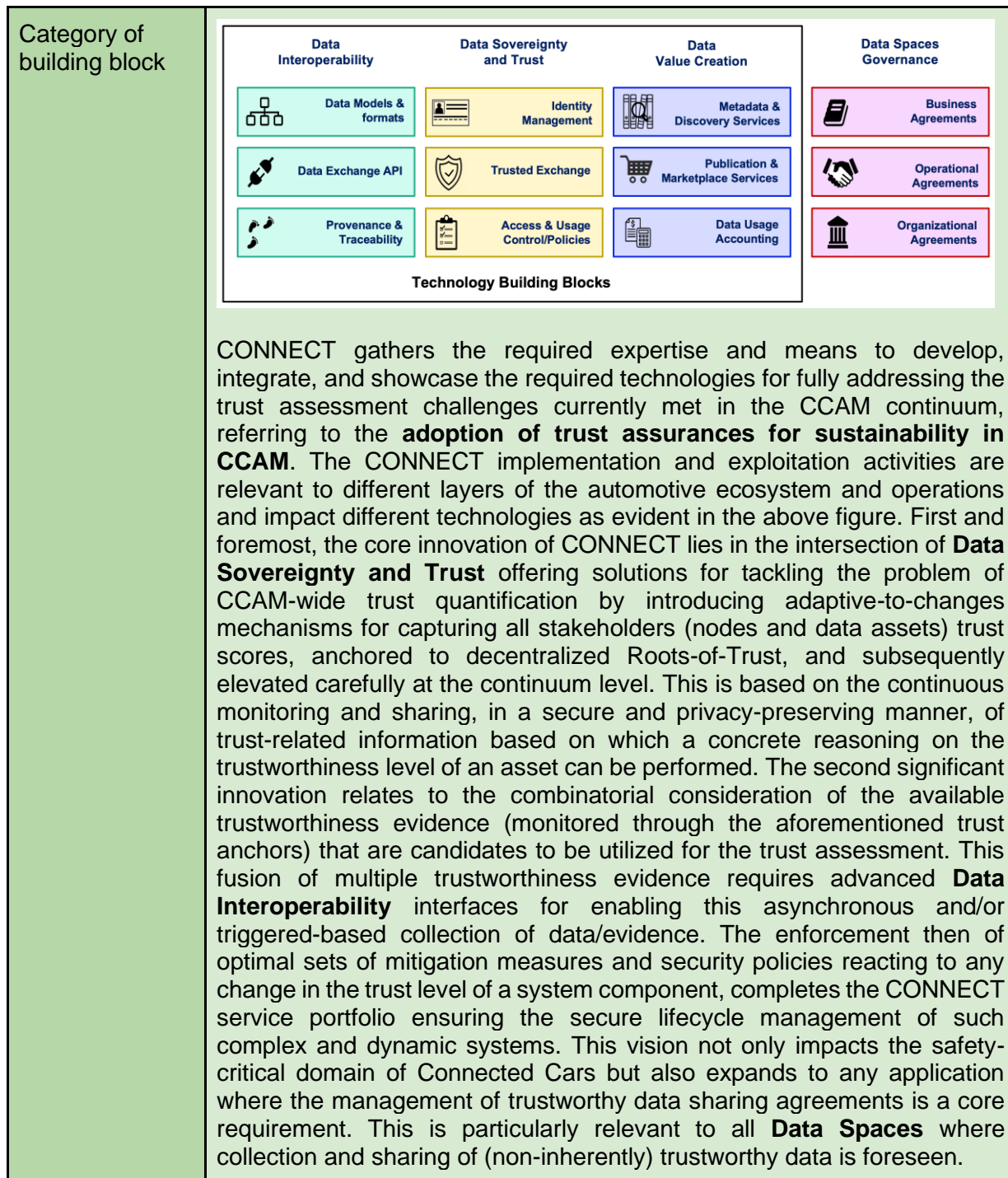


Table 8: CONNECT open-source project plan – context

3 Strategy											
3.1 Business											
Open-source canvas	<p>CONNECT has identified the following model: Co-creation of open-source extendible platforms</p> <table border="1"> <tr> <td><i>Key partner</i> Eclipse open-source communities</td> <td><i>Key activities</i> Platform maintenance and extension</td> <td><i>Value proposition</i> Trust assessment controls Subjective logic-based trust indicator Integration of trust assessment capabilities in the vehicle Introduction of MEC capabilities</td> <td><i>Customer relationships</i> Loose (indirect) Tight (specific partner collaboration)</td> <td><i>Users</i> V2X system developers</td> </tr> <tr> <td></td> <td><i>Key resources</i> Technology leader: Ubitech, Huawei Academic leader: UULM, SystemX</td> <td></td> <td><i>Channels</i> Open-source foundation V2X events</td> <td></td> </tr> </table>	<i>Key partner</i> Eclipse open-source communities	<i>Key activities</i> Platform maintenance and extension	<i>Value proposition</i> Trust assessment controls Subjective logic-based trust indicator Integration of trust assessment capabilities in the vehicle Introduction of MEC capabilities	<i>Customer relationships</i> Loose (indirect) Tight (specific partner collaboration)	<i>Users</i> V2X system developers		<i>Key resources</i> Technology leader: Ubitech, Huawei Academic leader: UULM, SystemX		<i>Channels</i> Open-source foundation V2X events	
	<i>Key partner</i> Eclipse open-source communities	<i>Key activities</i> Platform maintenance and extension	<i>Value proposition</i> Trust assessment controls Subjective logic-based trust indicator Integration of trust assessment capabilities in the vehicle Introduction of MEC capabilities	<i>Customer relationships</i> Loose (indirect) Tight (specific partner collaboration)	<i>Users</i> V2X system developers						
		<i>Key resources</i> Technology leader: Ubitech, Huawei Academic leader: UULM, SystemX		<i>Channels</i> Open-source foundation V2X events							
<table border="1"> <tr> <td><i>Cost structure</i> Key resource availability Participation of open-source foundation activities</td> <td><i>Revenue streams</i> Services and products built on top of platform</td> </tr> </table>	<i>Cost structure</i> Key resource availability Participation of open-source foundation activities	<i>Revenue streams</i> Services and products built on top of platform									
<i>Cost structure</i> Key resource availability Participation of open-source foundation activities	<i>Revenue streams</i> Services and products built on top of platform										
Assessment within project	<ul style="list-style-type: none"> ✓ Availability of software ✓ IPR approach finalised. ✓ Agreement with open-source foundation 										
Assessment beyond project	Implementation of business model										
3.2 Open-source licensing and IPR											
Current licensing and IPR status	The CONNECT Trust Extensions will be offered through the Apache 2.0 license. However, when the open-source development plans per exploitable asset will be constructed, other open-source license variants may also be explored depending on the needs and requirements of the technical partners involved.										
Analysis	<i>Provide an analysis of how you plan to enforce business-friendly licenses</i>										
Decisions within project	An enquiry (excel file) will be circulated within the project to finalise the IP agreement										
Decisions	None identified at this point										

beyond project			
3.3	Community approach		
Community	<u>Governance: open-source organisation, Development: community</u> The below identification of the TRL pertains to overarching CONNECT framework which, as aforementioned, comprises multiple technical components. This overall TRL value also depicts the maturity of the technology readiness level of the majority of the components – besides those components that are mirrored to their industrial equivalents including the Gramine TEE which the expected TRL at the end of the project will reach 8 (started from 6) and UBITECH's OLISTIC Risk Assessment with an expected TRL of 8 (started at 7).		
	Current status of KER	TRL	4
		Community	Open-Source
	Intended status at the end of project	TRL	6
		Community	Open-Source
	Intended status beyond project	TRL	Not decided yet
Community		Open-Source	
3.4	Governance		
Governance	Governance: open-source organisation, Development: community Lead Thanassis Giannetsos agiannetsos@ubitech.eu		
Decisions within project	Role of each partner Approach to engage external organisations		
Decisions beyond project	Function extensions to the developed platform		

Table 9: CONNECT open-source project plan – strategy

4	Engagement	
4.1	Stakeholders	
Developers	Current team	The CONNECT Framework implementation comprises of numerous activities that happen concurrently between all collaborating partners. Below is an indicative list of some team members focusing on the implementation of the concrete exploitable CONNECT artefacts: <ul style="list-style-type: none"> ✓ Trust Assessment Framework: UULM (Artur Hermann, Natasa Trkulja, Benjamin Erb), HUAWAI (Ana Petrovska, Koffi Ismael Ouattara); ✓ Risk Assessment Engine: UBITECH (Nikos Fotos,

		<p>Nikos Chatzivasileiadis), UULM (Artur Hermann), DENSO (Anderson Ramon Ferraz de Lucena)</p> <ul style="list-style-type: none"> ✓ Attestation Enablers: INTEL (Dmitrii Kuvaiskii, Matthias Schunter), UBITECH (Stefanos Vasileiadis, Vasilis Kalos, Thanassis Giannetsos, Benjamin Larsen), SURREY (Christofer Newton); ✓ Cryptographic Primitives: UBITECH (Stefanos Vasileiadis, Vasilis Kalos, Thanassis Giannetsos, Benjamin Larsen), SURREY (Christofer Newton); ✓ Runtime Tracer: INTEL (Dmitrii Kuvaiskii, Matthias Schunter), UBITECH (Stefanos Vasileiadis, Vasilis Kalos, Thanassis Giannetsos, Benjamin Larsen); ✓ Misbehaviour Detection: Francesca Bassi, Innes Ben Jemaa; ✓ MEC: ICCS (Pavlos Bassaras, Panagiotis Pantazopoulos); ✓ Blockchain: S5 (Kostas Latanis, Sotiris Kousouris)
	Team evolution during project	No change
	Team evolution beyond project	No change at this point
Users	Intended users	<p>The primary users to leverage and experiment with the CONNECT artefacts are the envisioned use cases. In particular:</p> <ul style="list-style-type: none"> ✓ IRTS-X in the case of Intersection Movement Assistance & Misbehaviour Detection where there is a need for combining heterogeneous sources of evidence to assess the trust indicator of incoming kinematic data; ✓ DENSO in the case of Cooperative Adaptive Cruise Control for keeping a safe distance to the vehicle in front based on the trust assessment of the exchanged data between neighbouring vehicles; ✓ CRF in the case of Slow-Moving Traffic Detection where the trustworthiness of data transmitted for non-connected ego vehicles need to be assessed by the backend Traffic Control System.
	External users during project	None identified at this point
Other stakeholders	Original Equipment Manufacturers (OEMs), Automobile Manufacturers, Automotive Suppliers, ITS Solution Providers, Telecom Industry, Mobile Network Operators, Cloud Providers, Fleet Operators, Transport Authorities, Road Authorities, Road Operators	
4.2	Activities	

Activities within project	List of standardization and dissemination activities as listed in D7.1 and also presented in Chapters 3 and 4. It is expected that CONNECT will engage in an open-source initiative through two channels. First open-source communities from existing foundations (e.g., ECLIPSE foundation), and secondly CCAM community (e.g., ETSI ITS WG5).
Activities beyond project	Trustworthy AI

Table 10: CONNECT open-source project plan – engagement

5 Project development	
5.1 Environment	
Platform	Gitlab
Decisions during project	CONNECT Gitlab
Decisions beyond project	Not yet identified
5.2 Development and release approach	
Development lifecycle	<p>CONNECT Approach to Development Lifecycle: The consortium has opted to base the CONNECT evaluation framework on the basic principles of the Validation and Verification (V&V) methodologies of software products. V&V methodologies, following up on the V model approach, cover the whole development cycle of a software product based on the active engagement of the demonstrators in multiple demonstration iterations, exposing them to incremental versions of the platform services and APIs and generating feedback loops, allowing the developers to improve their components and the platform as a whole.</p> <p>The application of V&V based methodologies addresses:</p> <ul style="list-style-type: none"> (a) verification, i.e., the discovery and elimination of defects, gaps in development and possible security issues, and (b) validation, i.e., the fulfilment of the stakeholders’ needs and the generation of the expected benefits. <p>The definition of the CONNECT evaluation framework should reply to the following questions:</p> <p><i>Is the CONNECT platform operating according to its specifications?</i> This question concerns the technical validation of the project and has to be answered by conducting a quantitative technical evaluation, e.g., testing technical parameters of system availability, functionality, security, and performance. The baseline is the platform reference architecture as defined in Deliverable 2.1 [1] and the technical work performed in WP2-WP5.</p> <p><i>Does CONNECT meet the defined objectives from the perspective of its users?</i> This question is closely related to product validation and business</p>

validation; the demonstrator partners are directly involved in replying to it. During product validation, the focus is on platform usability, user acceptance, user satisfaction, etc. During business validation, the focus is on the contribution to different KPIs of business interest, from direct costs (and time therefore) to the strategic objectives of the call, to other aspects such as perceived Quality of Service, level of trust, etc. The baseline is the use cases which have been defined in D2.1 [1] and will be further elaborated in D6.1.

CONNECT Technical Validation Approach: The ISO/IEC 25010:2011 [27] “Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models” proposes a set of models that better address the evaluation of the software quality.

The product quality model is composed of eight characteristics (which are further subdivided into 31 sub-characteristics) that relate to static properties of software and dynamic properties of the computer system. The model is applicable to both computer systems and software products.



ISO/IEC 25010:2011 - PRODUCT QUALITY MODEL

1. **Functional Suitability** - The degree to which the product provides functions that meet stated and implied needs when the product is used under specified conditions.
2. **Performance Efficiency** - The performance relative to the number of resources used under stated conditions.
3. **Compatibility** - The degree to which two or more systems or components can exchange information and/or perform their required functions while sharing the same hardware or software environment.
4. **Usability** - The degree to which the product has attributes that enable it to be understood, learned, used and attractive to the user, when used under specified conditions.
5. **Reliability** - The degree to which a system or component performs specified functions under specified conditions for a specified period.
6. **Security** - The degree of protection of information and data so that unauthorised persons or systems cannot read or modify them, and authorised persons or systems are not denied access to them.
7. **Maintainability** - The degree of effectiveness and efficiency with which the product can be modified.
8. **Portability** - The degree to which a system or component can be effectively and efficiently transferred from one hardware, software or other operational or usage environment to another.

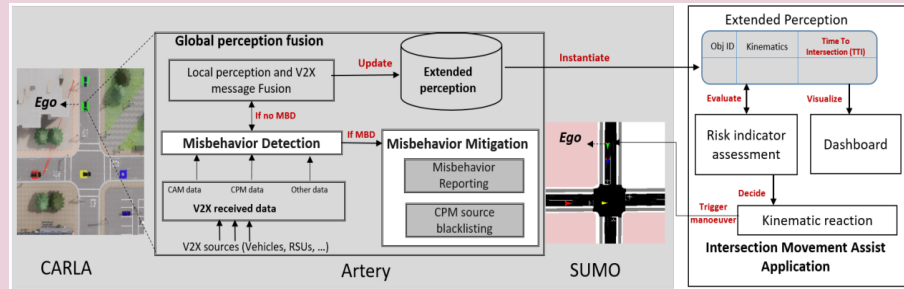
Sub-characteristics	Definition	Suitability for CONNECT

Functional Suitability		
Functional completeness	Degree to which the set of functions covers all the specified tasks and user objectives.	High
Functional correctness	Degree to which a product or system provides the correct results with the needed degree of precision.	High
Functional appropriateness	Degree to which the functions facilitate the accomplishment of specified tasks and objectives.	High
Performance Efficiency		
Time behaviour	Degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements. This is especially important in the context of CONNECT since we are dealing with CCAM environments providing safety-critical operations with strict time constraints.	High
Resource utilisation	Degree to which the amounts and types of resources used by a product or system, when performing its functions, meet requirements.	Medium
Capacity	Degree to which the maximum limits of a product or system parameter meet requirements.	Low
Compatibility		
Co-existence	Degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product. This is rather important in the context of CONNECT where all the security enablers are deployed at the edge devices for protecting the concurrent execution of the device computational tasks.	High
Interoperability	Degree to which two or more systems, products or components can exchange information and use the information that has been exchanged. In the context of CONNECT, this pertains to the data interoperability attributes for the attestation data recorded on the distributed ledger. It should be possible for an entity, with	High

	the appropriate privileges, to query/read from a ledger and then securely transfer this claim to another ledger for these registered devices to have access to.	
Usability		
Appropriateness recognisability	Degree to which users can recognize whether a product or system is appropriate for their needs.	High
Learnability	Degree to which a product or system can be used by specified users to achieve specified goals of learning to use the product or system with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use.	High
Operability	Degree to which a product or system has attributes that make it easy to operate and control.	High
User error protection	Degree to which a system protects users against making errors.	Low
User interface aesthetics	Degree to which a user interface enables pleasing and satisfying interaction for the user.	Low
Accessibility	Degree to which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use.	Low
Reliability		
Maturity	Degree to which a system, product or component meets needs for reliability under normal operation.	High
Availability	Degree to which a system, product or component is operational and accessible when required for use.	High
Fault tolerance	Degree to which a system, product or component operates as intended despite the presence of hardware or software faults.	High
Recoverability	Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.	High
Security		

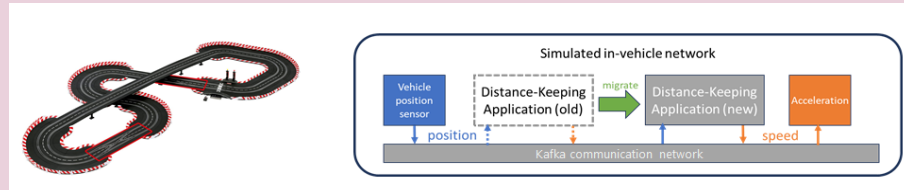
	Confidentiality	Degree to which a product or system ensures that data are accessible only to those authorised to have access based on their ability to exhibit specific attributes and partial identifiers.	High
	Integrity	Degree to which a system, product or component prevents unauthorised access to, or modification of, computer programs or data.	High
	Non-repudiation	Degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later.	High
	Accountability	Degree to which the actions of an entity can be traced uniquely to the entity.	High
	Authenticity	Degree to which the identity of a subject or resource can be proved to be the one claimed.	High
	Maintainability		
	Modularity	Degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components.	High
	Reusability	Degree to which an asset can be used in more than one system, or in building other assets.	Medium
	Analysability	Degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.	Low
	Modifiability	Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality.	Low
	Testability	Degree of effectiveness and efficiency with which test criteria can be established for a system, product or component and tests can be performed to determine whether those criteria have been met.	Medium
	Portability		

	Adaptability	Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.	High
	Installability	Degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment.	Low
	Replaceability	Degree to which a product can replace another specified software product for the same purpose in the same environment.	Low
Development lifecycle security assurance	Not decided yet		
Release building approach	Not decided yet		
Decisions during project	Not decided yet		
Decisions beyond project	Not decided yet		
5.3	Support		
Pilots involved	✓ The first Use Case of CONNECT concerns the Intersection Management Assist (IMA) application , a critical component in Intelligent Transportation Systems. An ego vehicle approaching an intersection, utilizes CAM messages to predict the trajectories of other vehicles, identifies potential collision zones, and issues timely warnings to the driver as collision probabilities reach predefined thresholds. More specifically, the vehicles in this Use Case employ a Local Dynamic Map (LDM) to predict the positions of dynamic objects in the intersection, primarily relying on information from CAM messages. The LDM, serves to store comprehensive information about the environment, encompassing both static and dynamic data. Addressing challenges related to legacy vehicles without communication capabilities, the introduction of the Collective Perception Service (CPS) complements CAM messages by periodically broadcasting Collective Perception Messages (CPMs). These CPMs enhance the LDM by providing information about dynamic objects perceived by the ego vehicle's on-board sensors, ensuring awareness of legacy vehicles.		




Details on the exact pilot to be demonstrated will be documented in D6.1 – although the focus will be on the evaluation of CONNECT through a simulation environment;

- ✓ Cooperative Adaptive Cruise Control (C-ACC) represents a cutting-edge application in the realm of intelligent transportation systems, enhancing traditional Adaptive Cruise Control through vehicle-to-vehicle communication. In this innovative use case, vehicles equipped with C-ACC exchange real-time messages, sharing crucial information such as current speed, acceleration, and position. This continuous communication allows the vehicles to operate in a coordinated manner, optimizing traffic flow and safety. We evaluate our use case within the framework of a **service-oriented zonal architecture**.



This architectural design features a zonal controller strategically positioned between the Electronic Control Unit (ECU) and the sensors and actuators, thereby facilitating the possibility of also enabling the delivery of specialized software updates. Our in-vehicle architecture consists of a smart antenna, enabling the communication with other vehicles, the Vehicle Computer, the zonal controllers and the sensors or actuators (i.e., lidar, etc.). For keeping a safe distance to the vehicle in front, the C-ACC bases its decisions on various data items received from in-vehicle sensors, as well as from other vehicles. Upon receiving the data, the C-ACC proceeds with making crucial driving decisions and generates two essential types of messages to ensure safe and coordinated driving: Acceleration command to the Acceleration ECU for regulating the vehicle’s speed (i.e., whether it should slow down or speed up) and CAM message to inform other vehicles about driving parameters, including speed, heading, etc. Details on the exact pilot to be demonstrated will be documented in D6.1 – although the experimentation and demonstration activities will revolve around the use of a toy track deployed at the premises of UULM;

- ✓ The Slow-Moving Traffic Detection (SMTD) system addresses traffic congestion by utilizing V2X communication technologies. It enables equipped vehicles to share real-time information about slow-moving vehicles on the road, enhancing road safety, reducing congestion, optimizing transport efficiency, and minimizing environmental impacts. Cooperative Perception Messages (CPMs) and Cooperative Awareness Messages (CAMs) play a crucial role, providing real-time environmental and kinematic data securely signed with short-term anonymous credentials. These messages could then be processed by a Mobile Edge Computing (MEC) server, acting as a central hub on the edge of the network for data analysis. The MEC server decodes the

	<p>incoming V2X messages and checks the correctness of the received data or for possible contradictions between multiple sources. The SMTD system focuses on real-time detection of slow-moving traffic, crucial for road safety and traffic management. Legacy vehicles lacking V2X capabilities rely on ADAS sensors for real-time detection, but without V2X, they cannot share this information.</p>  <p>Details on the exact pilot to be demonstrated will be documented in D6.1 – although the experimentation and demonstration activities will revolve around a real pilot leveraging the premises and equipped vehicle from CRF and POLITO.</p>
<p>Contact points pilot</p>	<ul style="list-style-type: none"> ✓ IRTSYSTEMX: Francesca Basi (francesca.bassi@irt-systemx.fr), Ines Ben Jemaa (ines.ben-jemaa@irt-systemx.fr) ✓ DENSO: Alexander Kiening (a.kiening@eu.denso.com) ✓ CRF/POLITO: Marco Zanzola (marco.zanzola@crf.it), Marco Rapelli (rapelli.m@libero.it)
<p>5.4</p>	<p>Evaluation</p>
<p>Schedule</p>	<p>CONNECT will follow a hybrid research and innovation methodology, building upon a best practice agile approach used in several complex R&D projects, extended, and refined by partners in-line with the needs of CONNECT. The process will start by collecting insights through stakeholders’/end-users’ activities (i.e., co-creation workshops), combined with information collected from linked research initiatives, relevant standards, and project-specific requirements. The resulting knowledge will be further analysed through requirements engineering techniques, leading to a set of requirements and innovation forms, each split into a set of prioritized platform functionalities. In the sequel, requirements and functionalities will be fed into the CONNECT requirements and innovation tracker, implemented on top of State of the Art (SotA) collaboration tools. The tracker will be used to make evident and transparent to all the consortium analysts and developers how many requirements are open, rejected or resolved and how many functionalities are defined, developed, or validated. The development activities are foreseen to occur based on two (2) main and intermediate software releases:</p> <p>First Iteration: This iteration starts with the baseline step comprising the activities of WP2 with regards to the delivery of high-level functional and non-functional requirements of the CONNECT Framework coupled with a first release of the overall conceptual architecture on M12. This includes a collaboration with all the technical WPs 3-5 for extracting the requirements, modes of operations and interfaces of all CONNECT internal modules: (i) Trust Assessment Framework (WP3), (ii) Harmonized Secure Elements (TEEs) for enabling “chip-to-cloud” assurances and establishing verifiable chains of trustworthy vehicles and RSUs (WP4), (iii) Distributed</p>

	<p>Processing, Fast Offloading through MEC Orchestration with Edge Computing capabilities and Digital Twins (WP5), (iv) Secure, Reliable Data Sharing through advanced crypto primitives (WP4, WP5), and (v) Trust Aware Continuous Authentication and Authorization capabilities through SSI-based Verifiable Credentials (WP5). This will lead to the detailed design (M15), implementation and testing of these standalone components (M18) prior to the release of the first integrated version of the CONNECT framework on M21 for detailed integration testing and evaluation.</p> <p>Second Iteration: The second iteration focuses mainly on updating the overall CONNECT trust assessment architecture based on any bugs or inconsistencies identified during the evaluation, conducted in the first phase, and the comments/feedback received by engaging the end-users on the explainability of the trustworthiness models, defined in the previous phase. This will lead to the finalization of the overall CONNECT architecture, published on M24, so that the final version of the internal modules can be implemented by M30, the final CONNECT integrated framework to be provided by M33, and the project impact assessment and end-user adoption guidelines to be produced at the end of the project M36.</p>
--	--

Table 11: CONNECT open-source project plan - project development

6	Evaluation and approval of plan
Project manager name	Thanassis Giannetsos agiannetsos@ubitech.eu
Approval date	February 8 th , 2024
Exploitation manager name	tbd
Approval date	tbd

Table 12: CONNECT open-source project plan - evaluation and approval of plan

Chapter 6 Exploitation, Business and Sustainability Planning

The initial statement on industrial/commercial involvement in the description of work was as follows (we have omitted Red Hat who has left the project):

Industrialization efforts will be primarily driven by the consortium large industries (INTEL, HUAWEI, DENSO, CRF), having proven experience in bringing products/solutions to the market, while possessing multinational sales/marketing channels and a footprint in standardization bodies. However, the project will also provide commercialization opportunities to the SMEs of the consortium, through:

- (i) Enabling them to enhance their existing products based on trusted computing, 4G/5G multi-connectivity, MEC concepts and relevant scientific insights (e.g., this is the case with UBITECH and S5),
- (ii) (Providing them new opportunities for developing new security (and other automotive) solutions for their customers/stakeholders (e.g., Extend the MBD System (IRTSX), Driver-assistance services and data monetization based on secure data lakes (CRF), Maintaining the Cooperative Intelligent Transport System in a safe condition throughout the life cycle of the vehicle (TRIALOG)), and
- (iii) Enable them to commercialize parts of CONNECT results that are involved (e.g., Trust Modelling and Digital Twins).

Overall, CONNECT acknowledges the importance of involving SMEs in cutting edge research and gives them the chance to commercialize such results.

The below table provides an update of the intentions of the partners at M18.

Partner	Initial position (at project start)	Current status (M18)
Technikon	Project management in innovation	Unchanged
Ubitech	Enhance existing products based on trusted computing	Open-source approach confirmed
Huawei	Industrialization effort Trust Modelling and Management, Hardware Security, Security Engineering, Trusted Execution Environment	Unchanged
ICCS	Advance in trust-aware network orchestration and secure data sharing	In-depth know-how of trusted containers technology and their incorporation into the ICCS (5G testbed) software infrastructure as well as research agenda
UUIIm	Advance on the use of subjective logic in CCAM	Unchanged
Trialog	Maintaining the Cooperative Intelligent Transport System in a safe condition throughout the life cycle of the vehicle	Same position with a view to integrate trustworthiness (e.g. AI). Using the potential open source
Denso	Industrialization effort V2X services	Unchanged
Intel	Industrialization effort Trust Modelling and Management, Hardware Security, Security	Focus on GRAMINE

	Engineering, Trusted Execution Environment	
Suite5	Enhance existing products based on trusted data sharing Advance know-how on blockchain technologies and smart contracts	Open-source approach confirmed Experimentation with different blockchain technologies for the selection of the CONNECT DLT blockchain technology
Unisystems	Integration know-how	Unchanged
U.Twente	Advance in ethics	Unchanged
FSCOM	Support on standardization Advance on application of subjective logic in CCAM	Continuation standardization Advance FSCOM testing know-how with security and subjective logic topic
CRF	Industrialization effort V2X services Driver-assistance services and data monetization based on secure data lakes	Unchanged
IRTSX	Advance on Misbehaviour Detection system	Unchanged
Surrey	Advance on the use of subjective logic in CCAM	Unchanged

Table 13: Industrialization efforts per CONNECT partner

Chapter 7 Workshop planning

CONNECT is planning to present its work and the resulting findings at a number of events. This will include the organization of CONNECT centred workshops for the dissemination of the CONNECT concepts and methodology with the practical demonstration of project results and the participation in international conferences with technical contributions and a project presence at the affiliated exhibitions.

The present deliverable gives an overview of the present considerations, deliverable D7.3, due at the end of the project, will have the full report on CONNECT achieved organization/participation in conferences and workshops.

Event Location Date	Planned activity
ITS WC 2024 Dubai (UAE) 16-20 Sep 2024 Special Interest Session	<p>The 30th ITS World Congress in Dubai is being coordinated by ERTICO – ITS Europe, with the backing of RTA Dubai as the hosting entity. The objective of the ITS Congress is to promote understanding and adoption of intelligent mobility solutions among policymakers, experts, and the public. The congress aims to facilitate engaging discussions among ITS professionals, offering a diverse program of over 200 technical sessions, alongside an international exhibition and demonstration area.</p> <p>CONNECT has applied for a Special Interest Session (SIS) with the title “Trustworthy Connected, Cooperative & Automated Mobility: From Idea to Technical Implementation.”</p> <p>The selection process is currently ongoing, and the results of the selection process will be published in April 2024.</p>
ITS WC 2024 Dubai (UAE) 16-20 Sep 2024 Stand presence	<p>In addition to the planned SIS described above, CONNECT is currently also considering a presence at the exhibition. The project understood that the EC will not be present at the event with its own stand and therefore CONNECT is investigating other ways to ensure its presence at a stand. There may be the possibility to have a presence of the stand of ERTICO - ITS Europe where already several other EU funded projects will be present.</p>
EUCAD Ispra (Italy) 13-15 May 2025	<p>The EUCAD 2025 conference will showcase cutting-edge research, policy initiatives, and regulatory advancements in the realm of Cooperative, Connected, and Automated Mobility (CCAM). It will highlight European projects and recent Research and Innovation (R&I) breakthroughs that bolster the adoption of CCAM solutions in the market. The Conference agenda will feature a blend of policy-focused sessions alongside technical discussions addressing pertinent R&I hurdles. Concurrently, attendees will have access to an exhibition showcasing European and national R&I CCAM projects, alongside live demonstrations, throughout the event.</p> <p>EUCAD 2025 is considered the ideal arena to present CONNECT results in a technical session and to have a presence at the exhibition to disseminate the CONNECT methodology and to demonstrate project results in the deployments of the use cases.</p> <p>CONNECT plans to be part of EUCAD 2025 and will make the necessary efforts i.e., submission of a project contribution to a technical session and investigation on the conditions for a CONNECT presence at the exhibition.</p>

<p>Workshop at CONNECT final event CRF premises Date (tbd)</p>	<p>CONNECT is envisioning the organization of a scientific workshop for presenting the final version of the overarching CONNECT Trust Assessment framework and all internal building blocks fully evaluated in the context of the use cases. This will also be coupled with the live demonstration of the Slow-Moving Traffic Detection pilot that will be conducted at the premises of CRF. The goal is to engage members and stakeholders from the automotive industry as well as policy makers but also an audience from standardization activities trying to increase the impact of CONNECT findings and innovations.</p>
--	---

Table 14: Target events for CONNECT participation

Chapter 8 Summary and Conclusion

The present deliverable summarizes the WP7 ‘Dissemination, Standardization, Exploitation & Impact Creation’ activities of the CONNECT project. This deliverable follows on D7.1 which was published in M6 and will be followed by D7.3 at the end of the project in M36. Consequently, D7.2 presents a snapshot of the activities at M18 i.e., at halftime of the CONNECT project.

Dissemination and communication activities are covered in chapter 2 showing that the strategy established in D7.1 is followed and that the defined dissemination KPIs and communication targets have been achieved.

Clustering and standardization activities show already a good coverage of relevant industry and standardization groups. Project partners are actively assisting in shaping the standardization landscape by participating in relevant SDO groups at ISO, IEC and ETSI. Notably, a CONNECT use case has already been contributed to ISO TC204 to become part of ISO TR12786. It is expected that with the maturing of the CONNECT results, further contributions will be possible in the relevant fields of research covered by CONNECT i.e., cybersecurity in ISO/IEC JTC1 SC27, digital twins in ISO/IEC JTC1 SC41, CCAM in ETSI TC ITS and MEC related in ETSI ISG MEC. Furthermore, CONNECT partners will continue their participation in the clustering groups listed in chapter 3 and will make further efforts to raise awareness of the CONNECT project and its results through the participation in meetings and the production of informative contributions such as white papers.

First work on open-source contributions and IPR handling has been performed and a first set of tables are introduced in chapter 5. This is for further study and project partners will fill further instances of the table set once the exploitable artefacts they develop have been fully developed.

Exploitation aspects are shortly covered in chapter 6 showing the development of the partners’ plans since the start of the project. It is expected that exploitation aspects will become of higher relevance with the completion of the development work towards the end of the project.

Currently, planning of workshops is focusing on three events, the ITS World Congress 2024, the EUCAD conference 2025 and a CONNECT workshop combined with the final event of the project.

Chapter 9 List of Abbreviations

Abbreviation	Translation
5GAA	5G Automotive Association
ACC	Adaptive Cruise Control
ADD	Direct Anonymous Attestation
AIOTI	Alliance for Internet of Things Innovation
ATL	Actual Trust Level
C-ITS	Cooperative-ITS
C2C-CC	CAR 2 CAR Communication Consortium
CCAM	Cooperative, Connected and Automated Mobility
CEN	European Committee for Standardization (Comité Européen de Normalisation)
CIV	Configuration Integrity Verification
DoA	Description of Action
EMDS	European Mobility Data Space
ETSI	European Telecommunications Standard
EU	European Union
F2F	Face to Face
GNSS	Global Navigation Satellite System
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IoV	Internet of Vehicles
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
JTC	Joint Technical Committee
MEC	Multi-access Edge Computing
OEM	Original Equipment Manufacturer
OSD	Open-Source Development
RTL	Required Trust Level
SDO	Standards Developments Organization

SIS	Special Interest Session
STF	Specialized Task Force
TAF	Trust Assessment Framework
TCG	Trusted Computing Group
TR	Technical Report
TS	Technical Specification
TSS	Trusted Software Stack
TTF	Testing Task Force
UC	Use Case
V2X	Vehicle-to-everything
WG	Working Group
WP	Work Package

Chapter 10 References

- [1] CONNECT, D2.1 "Operational Landscape, Requirements and Reference Architecture – Initial Version", 2023.
- [2] CONNECT, D3.1 "Architectural Specification of CONNECT Trust Assessment Framework, Operation and Interaction", 2023.
- [3] CONNECT, D7.1 "Plan for Dissemination and Exploitation incl. Communication", 2023.
- [4] 5GAA, "Cybersecurity for Edge Computing", 2023.
- [5] 5GAA, "Trustable Position Metrics for V2X Applications", Sept. 2023.
- [6] 5GAA, "Safety Treatment in Connected and Automated Driving Functions Report", Mar. 2021.
- [7] 5GAA, "Misbehaviour Detection White Paper", May 2022.
- [8] Sustainable Development Goals, <https://www.un.org/sustainabledevelopment/sustainable-development-goals/>
- [9] European Green Deal, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en
- [10] Sustainable and Smart Mobility Strategy, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0789>
- [11] Strategic Research and Innovation Agenda, <https://www.ccam.eu/wp-content/uploads/2023/11/CCAM-SRIA-Update-2023.pdf>
- [12] HORIZON-CL5-2021-D6-01, "Framework for coordination of Automated Mobility in Europe", <https://www.connectedautomateddriving.eu/about/fame/>
- [13] Towards a common European mobility data space, <https://mobilitydataspace-csa.eu/wp-content/uploads/2023/10/deliverable-3.1.pdf>
- [14] ISO/IEC, WD TS 27115, "Cybersecurity evaluation of complex systems — Introduction and framework overview", 2024 (working draft, not published).
- [15] ISO/IEC, PWI 27568, "Security and privacy of digital twins", 2022 (preliminary work item, not published).
- [16] ISO/IEC, CD 27090 "Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems", 2024 (committee draft, not published).
- [17] ISO/IEC, WD 27091 "Cybersecurity and Privacy — Artificial Intelligence — Privacy protection", 2023 (working draft, not published).
- [18] ISO/IEC, AWI 30188, "Digital Twin — Reference architecture", 2024 (new work item, not published).
- [19] ISO/IEC/IEEE, 42010, "Software, systems and enterprise — Architecture description", 2022.
- [20] ISO/IEC CD TS 30149 "Internet of things (IoT) — Trustworthiness principles", 2024 (committee draft, not published).
- [21] ISO/IEC, DIS 30141, "Internet of Things (IoT) — Reference architecture", 2024 (Draft international standard, not published).
- [22] ETSI, TS 102 940, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2", 2021.
- [23] ETSI, TS 103 759, "Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting service; Release 2", 2023.
- [24] ETSI, GS MEC 009, "Multi-access Edge Computing (MEC); General principles, patterns and common aspects of MEC Service APIs", 2021.
- [25] ETSI, CONNECT presentation at ETSI Security conference, "Road-Map Towards the Adoption of Dynamic Trust Assurances for Safety and Security Convergence in Safety-Critical Systems", 2023.

https://docbox.etsi.org/Workshop/2023/10_ETSISECURITYCONFERENCE/D41_5G/IRTSYS_TEMX_BASSI.pdf

- [26] ETSI, CONNECT presentation at ETSI IoT conference, “ISO/IEC JTC1/SC41 Digital Twins Activities”, 2023.

https://docbox.etsi.org/Workshop/2023/07_ETSIIoTCONFERENCE/S09_DIGITAL_TWINS/S_C41_ACTIVITIES_DIGITAL_TWINS_TRIALOG_KUNG.pdf

- [27] ISO/IEC, 25010, “Systems and software engineering; Systems and software Quality Requirements and Evaluation (SQuaRE); System and software quality models”, 2011.

Appendix A CONNECT Open-Source Project Plan Template

This template has been developed by Antonio Kung (Trialog) and has been reviewed by the ECLIPSE foundation (Rosaria Rossini and Philippe Krief) in the frame of the OpenContinuum support action³ to support IoT open-source development activities.

1 Open-source plan info	
Authors name and e-mail	<i>CONNECT persons in charge of providing and maintaining the plan. Can involve different partners.</i>
History	<i>The open-source plan can be updated several times, depending on how the status of its execution. Examples are: Change of strategy (e.g., modification of Key Exploitable Results (KER) objective, merging with another KER) Change in licencing approach Change in community approach Change in infrastructure use (e.g., Gitlab to Github)</i>
	Date
	Version
	Description of modification
Confidentiality	<i>You may wish to have up to three versions of the plan: Confidential at partner level (not provided to consortium) – However experience shows that it does not run Confidential at consortium and EC level (needed for deliverable) Public (needed for engagement)</i>

Table A1: Open-source project plan – open-source plan info

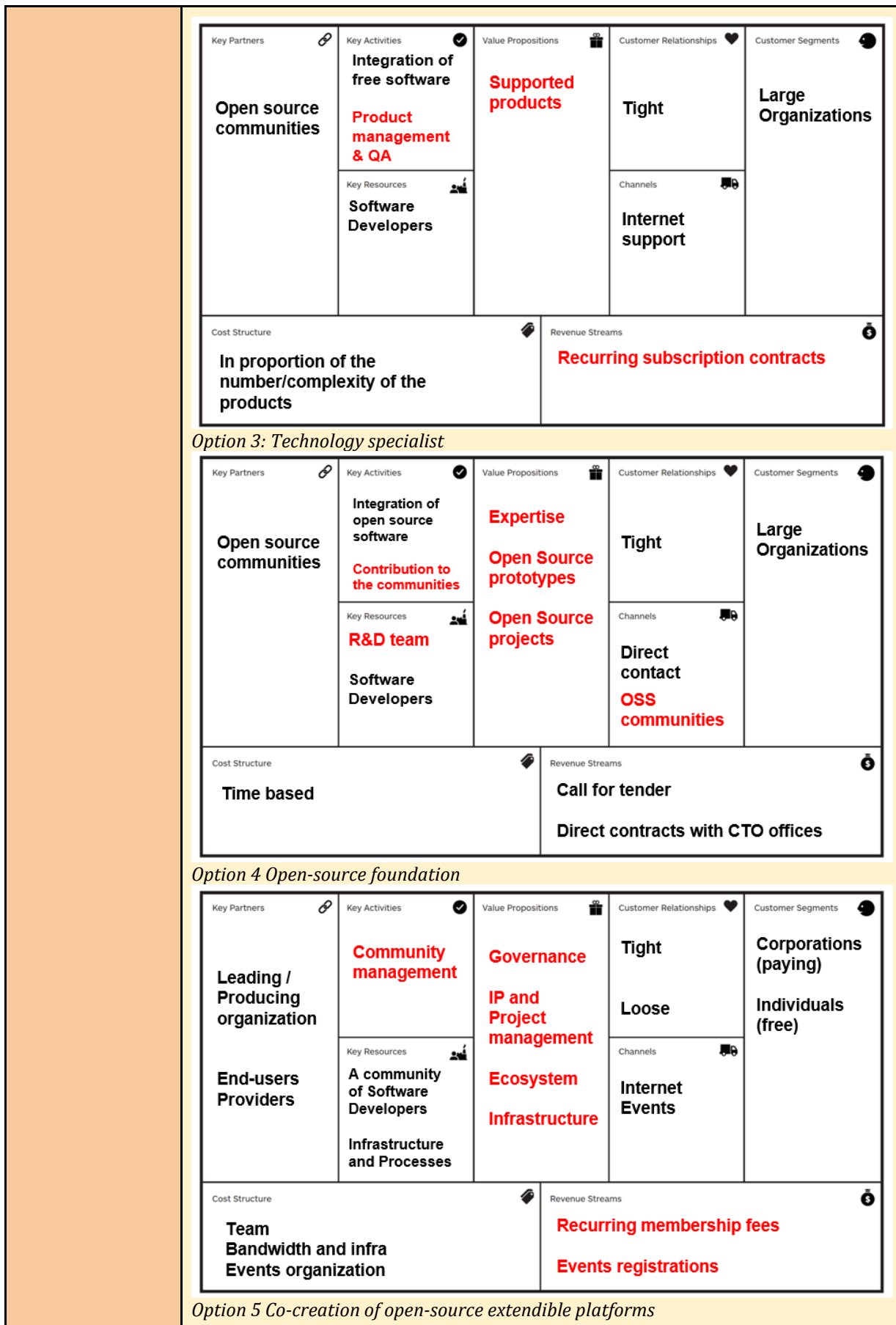
2 Context	
Initial Key exploitation result name	<i>Mention if you have modified your plans with respect to the grant agreement.</i>
Initial description	<i>Mention if you have modified your plans with respect to the grant agreement</i>
Key exploitation result name	
Description	<i>Provide a rationale for the change if you have modified your plans</i>

³ <https://eucloudedgeiot.eu/>

<p>Category of building block</p>	<p>Can you categorize the building block you are providing within a taxonomy of capabilities.</p> <p><i>Example below is from data space building blocks</i></p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <table border="1" style="width: 100%; text-align: center;"> <tr> <th style="width: 33%;">Data Interoperability</th> <th style="width: 33%;">Data Sovereignty and Trust</th> <th style="width: 33%;">Data Value Creation</th> <th style="width: 33%;">Data Spaces Governance</th> </tr> <tr> <td> Data Models & formats</td> <td> Identity Management</td> <td> Metadata & Discovery Services</td> <td> Business Agreements</td> </tr> <tr> <td> Data Exchange API</td> <td> Trusted Exchange</td> <td> Publication & Marketplace Services</td> <td> Operational Agreements</td> </tr> <tr> <td> Provenance & Traceability</td> <td> Access & Usage Control/Policies</td> <td> Data Usage Accounting</td> <td> Organizational Agreements</td> </tr> <tr> <td colspan="4">Technology Building Blocks</td> </tr> </table> </div> <p>How do you position your key exploitation results with respect to the 12 building blocks</p>	Data Interoperability	Data Sovereignty and Trust	Data Value Creation	Data Spaces Governance	Data Models & formats	Identity Management	Metadata & Discovery Services	Business Agreements	Data Exchange API	Trusted Exchange	Publication & Marketplace Services	Operational Agreements	Provenance & Traceability	Access & Usage Control/Policies	Data Usage Accounting	Organizational Agreements	Technology Building Blocks			
Data Interoperability	Data Sovereignty and Trust	Data Value Creation	Data Spaces Governance																		
Data Models & formats	Identity Management	Metadata & Discovery Services	Business Agreements																		
Data Exchange API	Trusted Exchange	Publication & Marketplace Services	Operational Agreements																		
Provenance & Traceability	Access & Usage Control/Policies	Data Usage Accounting	Organizational Agreements																		
Technology Building Blocks																					

Table A2: Open-source project plan – context

3	Strategy										
3.1	Business										
<p>Open-source canvas</p>	<p><i>Option 1: Major open-source initiative</i> <i>Provide a first version of the open-source canvas.</i> https://opensource.com/article/16/12/open-source-canvas</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%; padding: 5px;"> Problem What problem are you trying to solve for your users? Open source considerations Why is the solution open source? • To provide free offering? • To build up community? • Other reasons? </td> <td style="width: 25%; padding: 5px;"> Solution What is the solution? Open source considerations Independent versus Foundation? Which License? Activities What are the inbound and outbound activities you will carry out to encourage engagement with the project (e.g. conferences, blog posts, social media etc.)? </td> <td style="width: 25%; padding: 5px;"> Unique Value Proposition What is the promise of your project? Open source considerations Does the fact that it is open source contribute to the uniqueness of your offering? How? </td> <td style="width: 25%; padding: 5px;"> Community Relationships What are strategic relationships that are critical to building up your community? • Contributors • Project evangelists • Thought leaders • Integrations with other projects Channels Through which channels will you reach your users? • Collaboration partners who will distribute/expose project • Web, Social media etc. • Face to face (meetups, conferences etc.) </td> <td style="width: 25%; padding: 5px;"> Users Describe a typical user of your project Contributors Who are users that are most likely to contribute to your project – Super Users? </td> </tr> <tr> <td colspan="2" style="padding: 5px;"> Cost and Resources What human resources are required? Examples: • Project Maintainers (responsible for code governance etc.) • Paid engineers (core team to initiate the project or continue contributing) • Community Manager • Evangelist • Contributors to Community (not paid) Other costs? Examples: • Infrastructure/services • marketing </td> <td colspan="3" style="padding: 5px;"> Adoption Criteria How do you measure success of the project? Examples: • Size of community (number of issues/pull requests/stars etc.) • Number of contributors • Contributions (scale, variety, etc.) • Usage • Conversion rate (if your business model includes upgrade to enterprise version) </td> </tr> </table> <p style="font-size: small; text-align: center;">Open Source Canvas is adapted from the Business Model Canvas and the Lean Canvas and is licensed under Attribution-ShareAlike 4.0 International</p>	Problem What problem are you trying to solve for your users? Open source considerations Why is the solution open source? • To provide free offering? • To build up community? • Other reasons?	Solution What is the solution? Open source considerations Independent versus Foundation? Which License? Activities What are the inbound and outbound activities you will carry out to encourage engagement with the project (e.g. conferences, blog posts, social media etc.)?	Unique Value Proposition What is the promise of your project? Open source considerations Does the fact that it is open source contribute to the uniqueness of your offering? How?	Community Relationships What are strategic relationships that are critical to building up your community? • Contributors • Project evangelists • Thought leaders • Integrations with other projects Channels Through which channels will you reach your users? • Collaboration partners who will distribute/expose project • Web, Social media etc. • Face to face (meetups, conferences etc.)	Users Describe a typical user of your project Contributors Who are users that are most likely to contribute to your project – Super Users?	Cost and Resources What human resources are required? Examples: • Project Maintainers (responsible for code governance etc.) • Paid engineers (core team to initiate the project or continue contributing) • Community Manager • Evangelist • Contributors to Community (not paid) Other costs? Examples: • Infrastructure/services • marketing		Adoption Criteria How do you measure success of the project? Examples: • Size of community (number of issues/pull requests/stars etc.) • Number of contributors • Contributions (scale, variety, etc.) • Usage • Conversion rate (if your business model includes upgrade to enterprise version)		
Problem What problem are you trying to solve for your users? Open source considerations Why is the solution open source? • To provide free offering? • To build up community? • Other reasons?	Solution What is the solution? Open source considerations Independent versus Foundation? Which License? Activities What are the inbound and outbound activities you will carry out to encourage engagement with the project (e.g. conferences, blog posts, social media etc.)?	Unique Value Proposition What is the promise of your project? Open source considerations Does the fact that it is open source contribute to the uniqueness of your offering? How?	Community Relationships What are strategic relationships that are critical to building up your community? • Contributors • Project evangelists • Thought leaders • Integrations with other projects Channels Through which channels will you reach your users? • Collaboration partners who will distribute/expose project • Web, Social media etc. • Face to face (meetups, conferences etc.)	Users Describe a typical user of your project Contributors Who are users that are most likely to contribute to your project – Super Users?							
Cost and Resources What human resources are required? Examples: • Project Maintainers (responsible for code governance etc.) • Paid engineers (core team to initiate the project or continue contributing) • Community Manager • Evangelist • Contributors to Community (not paid) Other costs? Examples: • Infrastructure/services • marketing		Adoption Criteria How do you measure success of the project? Examples: • Size of community (number of issues/pull requests/stars etc.) • Number of contributors • Contributions (scale, variety, etc.) • Usage • Conversion rate (if your business model includes upgrade to enterprise version)									
<p><i>The other options are identified by ECLIPSE</i> <i>Option 2: Leveraged service business model</i></p>											



	<p>Option 6 e-Pure service business model</p>
Assessment within project	<i>Describe tasks to be carried out on business within the project</i>
Assessment beyond project	<i>Describe tasks that will be carried out on business beyond the project, make recommendations for a roadmap</i>
3.2	Open-source licensing and IPR
Current licensing and IPR status	<i>Explain the current status (e.g., the selected licensing plan) and the dependencies. See https://opensource.org/licenses (Licenses & Standards, s.d.) Describe decisions to be made on licensing and IPR within the project</i>
Analysis	<i>Provide an analysis of how you plan to enforce business-friendly licenses</i>
Decisions within project	<i>Describe decisions to be made on licensing and IPR within the project, justify when you do not select a well-accepted licensing scheme</i>
Decisions beyond project	<i>Describe decisions to be made on licensing and IPR beyond the project, justify when you do not select a well-accepted licensing scheme</i>
3.3	Community approach

Community	<p>Assess the intended community approach. Some references https://opensource.org/community (Community & Collaboration, s.d.), https://en.wikiversity.org/wiki/Open_community_approach (Open community approach, s.d.), https://www.linuxfoundation.org/resources/open-source-guides/participating-in-open-source-communities (Participating in Open Source Communities, s.d.), https://www.eclipse.org/collaborations/ (Industry Collaborations, s.d.)</p> <p>Example of community: Governance: single organisation, Development: single organisation Governance: single organisation, Development: community Governance: open-source organisation, Development: community</p>		
	Current status of KER	TRL	
		Community	
	Intended status at the end of project	TRL	
Community			
Intended status beyond project	TRL		
	Community		
Decisions within project	Describe decisions to be made on community approach within the project		
Decisions beyond project	Describe decisions to be made on community approach beyond the project		
3.4	Governance		
Governance	<p>Select the agreed open-source governance approach (see https://opensource.com/article/20/5/open-source-governance (What is open source project governance?, s.d.))</p>		
Decisions within project	Describe decisions to be made on community approach within the project		
Decisions beyond project	Describe decisions to be made on community approach beyond the project		

Table A3: Open-source project plan - strategy

4	Engagement	
4.1	Stakeholders	
Developers	Current team	List developers and their roles . Is the team involving several partners?
	Team evolution during project	Explain if the team will evolve during project
	Team evolution beyond project	Explain if the team will expand externally beyond the project, and how engagement will take place

Users	Intended users	List users (pilots) and their needs
	External users during project	<i>Explain if there will be external users during project, and how they will be engaged</i>
Other stakeholders	<i>List potential stakeholders that can have an interest to the project and need to be engaged</i> <i>Other open-source communities</i> <i>Platform / data space stakeholders</i> <i>Domain specific stakeholders (Consumers, local communities, data energy cooperatives)</i> <i>Energy and non-energy business stakeholders (finance, healthcare, water, mobility, etc.)</i> <i>Regulated operators</i> <i>Standardisation bodies</i>	
4.2	Activities	
Activities within project	<i>Inbound activities: liaison with other projects (through Int-Net, DSCC, OpenContinuum, and other Horizon projects), presentation to data space events (IoT, BDVA, BRIDGE, ...), conferences, blogs, ...</i> <i>Outbound activities: if any</i>	
Activities beyond project	<i>Inbound activities</i> <i>Outbound activities</i>	

Table A4: Open-source project plan – engagement

5	Project development	
5.1	Environment	
Platform	<i>List platforms and dependencies on other products or components</i>	
Development environment	<i>Explain development environment used to develop open-source project (e.g. Yocto)</i>	
Decisions during project	<i>Describe decisions to be made on environment during project</i>	
Decisions beyond project	<i>Describe decisions to be made on environment beyond project</i>	
5.2	Development and release approach	
Development lifecycle	<i>Explain lifecycle approach (development, verification et validation) and approach (e.g. DevOps) including tools to be used</i>	
Development lifecycle security assurance	<i>Explain measures for development lifecycle security assurance</i>	
Release building approach	<i>Explain approach including tools to be used</i>	
Decisions during project	<i>Describe decisions to be made on development and release during project</i>	

Decisions beyond project	<i>Describe decisions to be made on development and release beyond project</i>
5.3	Support
Pilots involved	
Contact points pilot	
Contact points KER	
Training material	
Training schedule	
5.4	Evaluation
Schedule	<i>Provide schedule for questionnaire to pilots, questionnaire to developers and evaluation report</i>

Table A5: Open-source project plan - project development

6	Evaluation and approval of plan
Project manager name	
Approval date	
Exploitation manager name	
Approval date	

Table A6: Open-source project plan - evaluation and approval of plan